G Data Business Software

User Manual

G Data. Security **Made in Germany.**

Inhaltsverzeichnis

G Data Business 3

Installation 7

G Data ManagementServer 31

G Data Administrator 32

G Data WebAdministrator 114

G Data MobileAdministrator 116

G Data Security Client 122

G Data MailSecurity MailGateway 128

G Data MailSecurity Administrator 130

G Data MobileSecurity 170

FAQ 180

G Data Business

In Zeiten der weltweiten Vernetzung und den daraus resultierenden massiven Sicherheitsrisiken, ist das Thema Virenschutz nicht länger nur für IT-Fachleute von Interesse. Es muss vielmehr im Rahmen eines umfassenden, unternehmensweiten Risikomanagements auf höchster Managementebene betrachtet werden. Ein durch Viren verursachter Ausfall des Computernetzwerks trifft ein Unternehmen an seiner empfindlichsten Stelle.

Die Folgen: Stillstand lebenswichtiger Systeme, Verlust erfolgsrelevanter Daten, Ausfall wichtiger Kommunikationskanäle. Computerviren können einem Unternehmen Schäden zufügen, von denen es sich nie mehr erholt!

G Data bietet Ihnen High-End Virenschutz für Ihr gesamtes Netzwerk. Die führende Sicherheitsleistung der G Data-Produkte wird seit Jahren in zahlreichen Tests mit Traumnoten prämiert. Die G Data Business-Software setzt konsequent auf zentrale Konfiguration und Verwaltung sowie größtmögliche Automatisierung. Alle Clients, ob Workstation, Notebook oder Fileserver, werden zentral gesteuert. Sämtliche Client-Prozesse laufen transparent im Hintergrund ab. Automatische Internet-Updates sorgen im Ernstfall einer Virenattacke für extrem kurze Reaktionszeiten.

Die zentrale Steuerung mit dem G Data ManagementServer ermöglicht Installation, Einstellungen, Updates, Fernsteuerung und Automatik für das gesamte Netzwerk. Das entlastet den Systemadministrator, spart Zeit und Kosten.

Wir wünschen Ihnen erfolgreiches und sicheres Arbeiten mit Ihrer G Data Business-Software.

Ihr G Data-Team

Versionsinformation

In dieser Dokumentation ist die Funktionalität aller G Data Business-Module beschrieben. Sollten Sie bei Ihrer installierten Software-Version ein Feature vermissen, können Sie über die **G Data Premium Hotline** bequem Informationen zum Upgrade Ihrer Software erhalten.

Copyright-Information

Copyright © 2013 G Data Software AG
Engine A: The Virus Scan Engine and the Spyware Scan Engines are based on BitDefender technologies © 1997-2013 BitDefender SRL.
Engine B: © 2013 Alwil Software
OutbreakShield: © 2013 Commtouch Software Ltd.
Patch management: © 2013 Lumension Security, Inc.
[G Data - 11.03.2013, 12:03]

G Data Business-Lösungen

Vom Endkunden über den Mittelstand bis hin zum Großunternehmen bietet G Data umfassenden Komplettschutz für jedes Netzwerk. Dank der neuesten Spitzentechnologie, genießen unsere Kunden höchstmögliche Sicherheit, beste Leistung in Verbindung mit optimaler Benutzerfreundlichkeit. Wählen Sie aus unseren Softwarepaketen Ihre maßgeschneiderte Lösung:

G Data ...	AntiVirus	Firewall	AntiSpam	Policy-Manager	BankGuard	Report-Manager	MobileDevice Management	MailSecurity	Backup
AntiVirus Business	★				★	★	★		
AntiVirus Enterprise	★		★		★	★	★	★	★
ClientSecurity Business	★	★	★		★	★	★		
ClientSecurity Enterprise	★	★	★		★	★	★	★	★
EndpointProtection Business (auch als Managed Service erhältlich)	★	★	★	★	★	★	★		
EndpointProtection Enterprise (auch als Managed Service erhältlich)	★	★	★	★	★	★	★	★	★
PatchManagement	Zusatzmodul für alle vorstehenden Business-Lösungen								
SmallBusiness Security	★	★	★		★	★	★	★	★

Hilfe-Dokumentation

Ausführliche Informationen zur Verwendung der Software finden Sie in der Programmhilfe, die Sie jederzeit über die Taste F1 kontextsensitiv öffnen können. Außerdem haben Sie die Möglichkeit, eine ausführliche PDF-Dokumentation im Downloadbereich der G Data Webseite herunterzuladen:

www.gdata.de

Internet-Ambulanz

Sollten Sie einen neuen Virus oder ein unbekanntes Phänomen feststellen, senden Sie uns in jedem Fall diese Datei über die Quarantäne-Funktion der G Data Software. Klicken Sie dazu im Bereich **Berichte** mit der rechten Maustaste auf einen Virusfund und wählen dort die Option **Quarantäne: Zur Internet-Ambulanz senden**. Wir analysieren den Virus und werden Ihnen möglichst schnell ein Gegenmittel zur Verfügung stellen. Selbstverständlich behandeln wir Ihre eingesandten Daten höchst vertraulich und diskret.

> Die Rücksende-Adresse für Antworten von der Internet-Ambulanz können Sie im Bereich **Optionen** > **Server-Einstellungen** > **E-Mail-Einstellungen** definieren.

PremiumHotline

Die **PremiumHotline** für G Data Netzwerklizenzen steht allen registrierten Business-Kunden jederzeit zur Verfügung.

> **Telefon: +49 234 9762 901**
> Nutzen Sie eine Flatrate, so ist das Supportgespräch nach den Tarifbedingungen ohne zusätzliche Kosten.
>
> **E-Mail: business-support@gdata.de**
>
> Viele Fragen und Sachverhalte sind auch schon im Supportbereich der G Data Website beantwortet worden. Besuchen Sie uns unter:
>
> **www.gdata.de**

Die Registriernummer finden Sie je nach Art des Produktes auf der Lizenzurkunde (MediaPack) oder in der Auftragsbestätigung. Kontaktieren Sie im Zweifelsfall Ihren Händler bzw. den betreuenden Distributor.

Überprüfen Sie vor Gesprächen mit der Hotline, wie Ihr Computer/Netzwerk ausgestattet ist. Wichtig sind dabei vor allem folgende Informationen:

- Die **Versionsnummern** des G Data Administrators und des G Data ManagementServers (diese finden Sie im **Hilfe**-Menü des G Data Administrators)
- Die **Registrierungsnummer** oder den **Benutzernamen** für das Internet-Update
- Die genaue Windows-Version (Client/Server)
- Zusätzlich installierte Hard- und Softwarekomponenten (Client/Server)

- Eventuell auftretende Fehlermeldungen (inkl. Fehlercodes, sofern vorhanden) im genauen Wortlaut

Mit diesen Angaben wird das Gespräch mit den Support-Mitarbeitern kürzer, effektiver und erfolgreicher verlaufen. Wenn möglich, platzieren Sie das Telefon in der Nähe eines Rechners, auf dem der G Data Administrator installiert ist.

Installation

Starten Sie Windows und legen die G Data DVD in Ihr DVD-Laufwerk ein. Es öffnet sich automatisch ein Installationsfenster. Schließen Sie alle anderen Programme, bevor Sie mit der Installation der G Data Software beginnen. Es kann zu Fehlfunktionen oder einem Abbruch kommen, falls z.B. Programme geöffnet sind, die auf Daten zugreifen, die die G Data Software zur Installation benötigt. Nachdem Sie die Schaltfläche **Installieren** gedrückt haben, erscheint ein Bildschirm, in dem Sie auswählen können, welche der G Data Software-Komponenten Sie installieren wollen. Folgende Installationsmöglichkeiten stehen zur Verfügung:

G Data Setup
Wählen Sie die zu installierende Komponente.
G Data ManagementServer
Der ManagementServer kontrolliert und steuert alle Clients auf Workstations, Notebooks oder File-Servern und versorgt diese mit Updates der Virensignaturen. Die Installation beinhaltet den G Data Administrator.
G Data BootCD Wizard
Mit Hilfe des BootCD Wizards können Sie eine bootfähige CD zur Basisvirenanalyse erstellen. Dazu werden die aktuellen Virensignaturen verwendet.
G Data Administrator
Der Administrator ist die Steuerungssoftware für den ManagementServer. Er kann von einem beliebigen Rechner im Netz gestartet werden.
G Data WebAdministrator
Der WebAdministrator ist eine Web-basierende Steuerungssoftware für den ManagementServer. Er kann mit Hilfe eines Web-Browsers gestartet werden.
G Data Security Client
Die Client-Software stellt den Virenschutz für die Clients her und führt die Jobs vom ManagementServer ohne Benutzeroberfläche im Hintergrund aus.
G Data MobileAdministrator
Der MobileAdministrator ist eine Web-basierende Steuerungssoftware für den ManagementServer. Er kann mit Hilfe eines Mobile-Web-Browsers gestartet werden.
G Data InternetSecurity
Die InternetSecurity-Software schützt nicht vernetzte Rechner mit Internetzugang.
Schließen

- **G Data ManagementServer**: Als erstes sollte der G Data ManagementServer auf dem Computer installiert werden, der alle G Data - relevanten Einstellungen und Updates verwalten soll. Der G Data ManagementServer ist das Herzstück der G Data Architektur: Er verwaltet die Clients, fordert neueste Software- und Virensignaturupdates automatisch vom G Data UpdateServer an und steuert den Virenschutz im Netzwerk. Mit der Installation des G Data ManagementServers wird automatisch auch die G Data Administrator-Software installiert, mit der der G Data ManagementServer gesteuert wird.

- **G Data Administrator**: Der G Data Administrator ist die Steuerungssoftware für den G Data ManagementServer, die die Verwaltung von Einstellungen und Updates für alle im Netzwerk installierten G Data - Clients ermöglicht. Der G Data Administrator ist passwortgeschützt und kann auf jedem Windows-Rechner installiert und gestartet werden, der übers Netzwerk mit dem G Data ManagementServer verbunden ist.

- **G Data Security Client**: Die Client-Software stellt den Virenschutz für die Clients bereit und führt die ihm vom G Data ManagementServer zugewiesenen Jobs ohne eigene Bedienoberfläche im Hintergrund aus. Die Installation der Client-Software erfolgt in der Regel zentral für alle Clients über den G Data Administrator.

- **G Data InternetSecurity**: Wenn Sie die SmallBusiness-Versionen der G Data Software nutzen, steht Ihnen die G Data InternetSecurity als zusätzlicher autonomer Schutz für Rechner zur Verfügung, die nicht mit Ihrem Netzwerk verbunden sind, z.B. Notebooks von Außendienstmitarbeitern. Diese Software beinhaltet eine umfangreiche eigene Hilfedokumentation.

- **G Data MailSecurity**: Die G Data MailSecurity sichert - vom Systemadministrator zentral gesteuert - den gesamten SMTP- und POP3 basierten E-Mailverkehr mit und in Ihrem gesamten Netzwerk. Wenn Sie eine Enterprise-Version der G Data Software verwenden, steht Ihnen die G Data MailSecurity zur Installation zur Verfügung.

- **G Data BootCD Wizard**: Mit Hilfe des G Data BootCD Wizards können Sie eine bootfähige CD zur grundlegenden Überprüfung Ihres Rechners erstellen. Diese Überprüfung findet noch vor dem Start des installierten Betriebssystems statt. Dazu werden die aktuellen Virensignaturen verwendet. Mit einer erstellten G Data BootCD können Sie einen BootScan auch ohne die Original G Data-Software-DVD durchführen. Lesen Sie hierzu auch das Kapitel **G Data BootCD**.

- **G Data WebAdministrator**: Der G Data WebAdministrator ist eine webbasierte Steuerungssoftware für den G Data ManagementServer. Mit ihm können Einstellungen für den G Data ManagementServer über ein Webinterface in einem Browser vorgenommen werden. Er kann auf diese Weise ein Ersatz für die Installation des G Data Administrators sein.

- **G Data MobileAdministrator**: Der MobileAdministrator ist eine Web-basierende Steuerungssoftware für den ManagementServer. Er kann mit Hilfe eines Mobile-Web-Browsers gestartet werden und bietet Ihnen grundlegende Administrationsfunktionen des G Data Administrators. Der MobileAdministrator steht Ihnen bei den Programmversionen AntiVirus, ClientSecurity und EndpointProtection (Business/Enterprise) zur Verfügung.

Erste Schritte

Führen Sie bei akutem Virenverdacht auf den betroffenen Rechnern erst einen **G Data BootScan** durch.

1. Installieren Sie den **G Data ManagementServer** auf Ihrem Server. Bei der Installation des G Data ManagementServers wird automatisch der **G Data Administrator** auf dem Server installiert. Mit diesem Programm kann der G Data ManagementServer gesteuert werden. Um den optimalen Schutz zu gewährleisten, sollte der Rechner immer erreichbar (eingeschaltet) sein und für das automatische Laden der Virensignaturen über einen Internetzugang verfügen. Eine Installation des G Data ManagementServers muss nicht auf einem Serverbetriebssystem erfolgen (siehe **Systemvoraussetzungen**).

2 Führen Sie nun die Online-Registrierung durch. Ohne eine Online-Registrierung können keine Aktualisierungen der Software und der Antivirensignaturen erfolgen.

3 Beim ersten Start des G Data Administrators auf dem Server startet der **Einrichtungsassistent**. Mit diesem kann die **Client-Software** auf den gewünschten Clients in Ihrem Netzwerk auch über eine Remote-Installation verteilt und eingespielt werden. Alle Einstellungen, die mit dem Einrichtungsassistenten vorgenommen werden, lassen sich auch nachträglich ändern.

> Sollten sich Probleme bei der Remote-Installation der Clients ergeben, kann die Client-Software auch über eine Active Directory Synchronisierung eingespielt werden oder lokal auf dem jeweiligen Client mit Hilfe der G Data DVD oder einem selbst erstellten Client-Installationspaket installiert werden. Client-Installationspakete können auch über GPO/Anmelde-Skripte verteilt werden. Damit auch der Server selbst vor Virenbefall geschützt ist, empfiehlt sich auch für den Server die Installation der Client-Software.

4 Nach erfolgter Einrichtung und Installation der Client-Software auf den angeschlossenen Maschinen kann der Virenschutz sowie die Internet-Updates der G Data Client- und Serversoftware zentral gesteuert werden. Der G Data Administrator bietet unter anderem Einstellungsmöglichkeiten für den Echtzeitschutz durch den **G Data Wächter** sowie die Möglichkeit, Scanaufträge zu definieren, die das Netzwerk regelmäßig auf Virenbefall untersuchen.

> Sollte es notwendig werden, ein Einstellungsproblem an einem Client vor Ort zu lösen, kann der G Data Administrator auf jedem Client innerhalb des Netzwerks installiert werden. Damit entfällt die Notwendigkeit, alle Einstellungen lokal am Server vorzunehmen. Sollte es notwendig werden eine kritische Situation innerhalb Ihre Netzwerk außerhalb Ihre Unternehmen zu lösen, kann der **G Data WebAdministrator** über jeden Desktop-Web-Browser verwendet werden. Mit dem **G Data MobileAdministrator** können Sie die Administration so unterwegs von Ihren Mobile-Web-Browser aus durchführen.

Systemvoraussetzungen

Folgende Mindestanforderungen werden an die Clients- bzw. Server gestellt:

Enterprise Produkte und SmallBusiness Security

G Data ManagementServer/Security Client/MailSecurity (32-bit/64-bit)

Windows 8/Windows 7/Windows Vista/Windows XP SP3 (32-bit)

Windows Server 2012/Windows Server 2008/Windows Server 2003

mit mindestens 1 GB verfügbarem Arbeitsspeicher.

Empfohlene Systemvoraussetzung für den Betrieb des G Data ManagementServers:

Multicore CPU mit mindestens 4 GB verfügbarem Arbeitsspeicher.

G Data MailSecurity (Microsoft Exchange Plugin 64-bit)

Microsoft Exchange Server 2010/Microsoft Exchange Server 2007 SP1

Business Produkte (ohne MailSecurity)

G Data ManagementServer/SecurityClient (32-bit/64-bit)

Windows 8/Windows 7/Windows Vista/Windows XP SP3 (32-bit)

Windows Server 2012/Windows Server 2008/Windows Server 2003

mit mindestens 1 GB verfügbarem Arbeitsspeicher.

Das G Data-System nutzt das TCP/IP-Protokoll zur Kommunikation von Client- und Server-Rechnern untereinander.

Port-Konfiguration

Die G Data Produkte nutzen unterschiedliche TCP Ports zur sicheren Kommunikation innerhalb Ihres Netzwerks. Bitte stellen Sie sicher, dass diese Ports in Ihrer Firewall entsprechend freigegeben sind:

Main-Server (MMS)

- Port 7161 (TCP): Kommunikation zwischen Clients und Subnet-Servern
- Port 7182 (TCP): Kommunikation mit dem G Data Administrator
- Port 7183 (TCP): Kommunikation mit mobilen Clients
- Port 7184 (TCP): Kommunikation mit mobilen Clients (Distribution der Installationsdateien für mobile Clients)

Subnet-Server

- Port 7161 (TCP): Kommunikation mit Clients und Subnet-Servern

Clients

- Port 7167 (TCP): Kommunikation mit (Subnet)-Servern
- Port 7169 (TCP): Kommunikation mit Clients (peer-to-peer Update-Distribution)

Wenn Sie das Microsoft Exchange Plugin der G Data MailSecurity nutzen, stellen Sie bitte sicher, den Port 7171 (TCP) auf dem Rechner zu konfigurieren, auf dem das Plugin installiert ist, damit die Kommunikation zwischen Plugin und Main-Server gewährleistet ist.

Ports ändern

Die Portnummern wurden für die G Data Software so ausgewählt, um Konflikte mit bestehenden Standardanwendungen zu vermeiden. Sollte es dennoch zu Port-Konflikten kommen, können Sie die Ports des G Data ManagementServers natürlich entsprechend ändern. Öffnen Sie dazu zuerst den Services Control Manger (**Start**, **Run**, *services.msc*) mit Administrator-Rechten und stoppen Sie den G Data ManagementServer Hintergrund-Task. Öffnen Sie nun im Installationsordner Ihres G Data Produktes (typischerweise C:\Program Files\G DATA\G DATA AntiVirus ManagementServer) die Datei *gdmms.exe.config* in einem Text-Editor (z.B. Notepad). Hinterlegen Sie Sie nun - falls notwendig - für die folgenden Einträge geänderte Portnummern:

- **AdminPort**: Geben Sie hier die gewünschte Portnummer ein. Der Standardwert ist hier "0" (d.h. der Port bliebe dann voreingestellt auf 7182).
- **ClientHttpsPort**: Der Standardwert ist hier "0" (d.h. der Port bliebe dann voreinstellt auf 7183). In der Regel sollte der ClientHttpsPort-Wert nicht geändert werden, da mobile Clients keinen alternativen Port akzeptieren.
- **ClientHttpPort**: Geben Sie hier die gewünschte Proxy-Nummer ein. Der Standardwert ist hier "0" (d.h. der Port bliebe dann voreingestellt auf 7184).

Wenn Sie die Werte für den ClientHttpPort oder den ClientHttpsPort ändern, müssen Sie die HTTP-Sicherheitskonfiguration für den jeweiligen Port neu initialisieren. Öffnen Sie dazu die Kommandozeile mit Administrator-Rechen und starten Sie *C:\Program Files\G DATA\G DATA AntiVirus ManagementServer\gdmmsconfig.exe /installcert*.

Führen Sie einen Neustart des G Data ManagementServers durch, nachdem Sie die Ports geändert haben. Bitte beachten Sie: Falls Sie den AdminPort geändert haben, müssen Sie bei jedem Einloggen beim G Data Administrator den geänderten Port angeben. Dies erfolgt in folgendem Format: *servername:port.*

G Data BootCD

Die G Data BootCD erlaubt eine Bekämpfung von Viren, die sich vor der Installation der Antivirensoftware auf dem Rechner eingenistet haben und möglicherweise die Installation der G Data Software unterbinden möchten. Dazu gibt es eine spezielle Programmversion der G Data Software, die schon vor dem Systemstart ausgeführt werden kann.

1a **Mit der Programm-DVD**: Legen Sie die G Data Software DVD in das Laufwerk. Klicken Sie auf dem sich öffnenden Startfenster auf **Abbrechen** und schalten Sie den Computer aus.

1b **Mit selbst erstellter G Data BootCD**: Hierzu muss zunächst das Erstellungsprogramm für die G Data BootCD installiert werden. Dies muss auf einem System erfolgen, auf dem ein G Data Security Client mit aktuellen Signaturen installiert ist. Folgen Sie bitte nach der Installation den Anweisungen des G Data BootCD Wizards, um eine **BootCD zu erzeugen**.

2 Starten Sie den Computer neu. Es erscheint das Startmenü der G Data BootCD.

3 Wählen Sie mit den Pfeiltasten die Option **G Data BootCD** und bestätigen die Auswahl mit **Enter**. Es wird nun ein Linux-Betriebssystem von der CD/DVD gestartet und es erscheint eine G Data Spezialversion für BootScans.

Falls Sie Probleme mit der Ansicht der Programmoberfläche haben, starten Sie den Rechner erneut und wählen bitte die Option **G Data BootCD – Alternative** aus.

4 Das Programm schlägt nun vor, die Virensignaturen zu aktualisieren. Klicken Sie hier auf **Yes** und führen Sie das Update durch. Sobald die Daten über das Internet aktualisiert wurden, erscheint die Meldung **Update complete**. Verlassen Sie nun den Update-Bildschirm mit Anklicken der **Close**-Schaltfläche.

> Das automatische Internet-Update steht Ihnen dann zur Verfügung, wenn Sie einen Router verwenden, der IP-Adressen automatisch vergibt (DHCP). Sollte das Internet-Update nicht möglich sein, können Sie den BootScan auch mit alten Virensignaturen durchführen. Dann sollten Sie allerdings nach der Installation der G Data Software möglichst bald einen neuen BootScan mit aktualisierten Daten durchführen. Wenn Sie eine G Data BootCD selbst erstellt haben, sind die Virensignaturen auf dem Updatestand, den der G Data Security Client zum Zeitpunkt der Erstellung der BootCD geladen hat.

5 Nun sehen Sie die Programmoberfläche. Klicken Sie auf den Eintrag **Check Computer** und Ihr Computer wird auf Viren und Schadsoftware untersucht. Dieser Vorgang kann je nach Rechnertyp und Festplattengröße eine Stunde oder länger dauern.

6 Sollte die G Data Software Viren finden, entfernen Sie diese mit Hilfe der im Programm vorgeschlagenen Option. Nach einer erfolgreichen Entfernung des Virus steht Ihnen die Originaldatei weiter zur Verfügung.

7 Nach Abschluss der Virenüberprüfung klicken Sie auf die **Exit**-Schaltfläche (unten rechts in der Linux-Programmoberfläche) und wählen anschließend **Restart** aus.

8 Entfernen Sie die G Data BootCD aus dem Laufwerk.

9 Schalten Sie ihren Computer wieder aus und starten Sie ihn erneut. Nun startet Ihr Computer wieder mit Ihrem Standard-Betriebssystem. Die G Data Software kann nun auf einem virenfreien System installiert werden.

G Data BootCD erstellen

Um eine G Data BootCD zu erstellen müssen Sie zunächst den G Data BootCD-Assistenten installieren. Dies sollte auf einem System erfolgen, auf dem ein G Data Security Client mit aktuellen Virensignaturen läuft. Legen Sie die G Data DVD ins Laufwerk und klicken Sie auf die **Installieren** Schaltfläche. Wählen Sie nun **G Data BootCD Wizard** aus.

G Data BootCD Wizard
BootCD Wizard
Willkommen!
Der BootCD-Wizard unterstützt Sie bei der Erstellung einer bootfähigen CD.
Diese CD wird automatisch bei Systemstart geladen und prüft Ihren Rechner auf Schädlinge, ohne dass Ihr eigentliches Betriebssystem gestartet wird.
< Back
Next >
Cancel

Nach Abschluss der Installation können Sie unter **Start** > **(Alle) Programme** > **G Data** > **G Data BootCD Wizard** mit einem Klick auf **BootCD erstellen** assistentengestützt eine BootCD erzeugen. Bitte achten Sie darauf, ein Virensignatur-Update durchzuführen, damit die BootCD die neuesten Antiviren-Signaturen enthält. Danach können Sie die BootCD erzeugen, indem Sie dieses auf CD brennen oder als ISO-Image speichern. Das ISO-Image kann dann ggf. übers Netzwerk an die Clients distribuiert werden.

CD/DVD Boot-Option im BIOS einstellen

Sollte das System nicht von CD/DVD-ROM booten, kann es sein, dass diese Option erst eingestellt werden muss. Dies erfolgt im BIOS, einem System, das noch vor Ihrem Betriebssystem gestartet wird. Um hier Änderungen vorzunehmen, führen Sie folgende Schritte durch:

1. Schalten Sie den Computer aus.
2. Starten Sie Ihren Computer wieder. Üblicherweise gelangen Sie zum BIOS-Setup, indem Sie beim Hochfahren (= Booten) des Rechners die **Entf**-Taste (manchmal auch die Taste **F2-** oder **F10-Taste**) drücken. Die Dokumentation des Rechnerherstellers liefert hierzu weitere Hinweise.

3 Wie Sie die Einstellungen in Ihrem BIOS-Setup im Einzelnen ändern, entnehmen Sie der Dokumentation Ihres Mainboard-Herstellers. Im Ergebnis sollte die Bootreihenfolge **CD/DVD-ROM**, **C:** lauten, d.h. das CD/DVD-ROM-Laufwerk wird zum **1st Boot-Device** und die Festplatten-Partition mit Ihrem Windows-Betriebssystem zum **2nd Boot-Device**.

4 Speichern Sie die Änderungen und starten Sie Ihren Computer neu. Jetzt ist Ihr Computer bereit für einen BootScan.

Installation des G Data ManagementServers

Legen Sie die G Data-DVD ein und drücken Sie die Schaltfläche **Installieren**. Wählen Sie anschließend die Komponente **G Data ManagementServer** durch einen Klick auf die nebenstehende Schaltfläche.

Schließen Sie spätestens jetzt alle offenen Anwendungen in Ihrem Windows-System, da diese sonst zu Problemen bei der Installation führen können. Lesen Sie sich nun die Lizenzvereinbarung zur Nutzung dieser Software durch. Wählen Sie **Ich akzeptiere die Bedingungen der Lizenzvereinbarung** und klicken dann auf **Weiter**, wenn Sie den Vereinbarungen in dieser Form zustimmen. Der nächste Bildschirm ermöglicht Ihnen die Auswahl des Installationsordners.

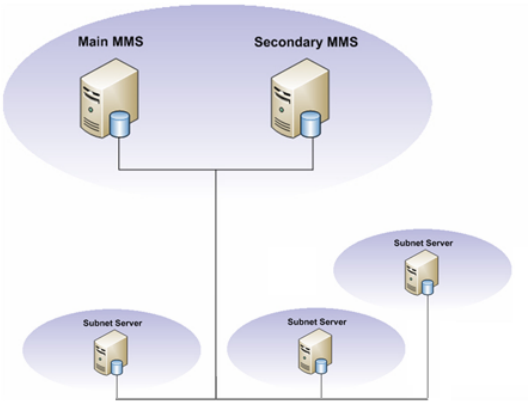
Server-Typ auswählen

Sie haben bei der Auswahl der Server-Typen folgende Optionen:

- **Einen Main-Server installieren**: Bei einer Erstinstallation muss der G Data ManagementServer immer als **Main-Server** (**Main-MMS**) installiert werden. Der Main-Server stellt die zentrale Konfigurations- und Verwaltungsinstanz der netzwerkbasierten Virenschutz-Architektur dar. Die zu schützenden Rechner werden über den G Data ManagementServer mit den jeweils aktuellsten Virensignatur- und Programmupdates versorgt. Darüber hinaus werden sämtliche Client-Einstellungen zentral am G Data ManagementServer vorgenommen.
- **Einen Secondary-Server installieren**: Bei Verwendung einer **SQL-Datenbank** ist es möglich, einen **zweiten Server** (**Secondary-MMS**) zu betreiben, der auf die gleiche Datenbank wie der Hauptserver zugreift. Falls der **Main-Server** eine Stunde oder länger nicht erreichbar ist, werden die Clients sich automatisch mit dem Secondary-Server verbinden und von diesem Signaturupdates laden. Der Wechsel zurück zum Hauptserver erfolgt, sobald dieser wieder verfügbar ist. Beide Server laden die Signaturupdates unabhängig voneinander und stellen so eine Ausfallsicherheit her.

- **Einen Subnet-Server installieren**: Bei großen Netzwerken (z.B. Firmenzentrale mit angeschlossenen Zweigstellen) kann es sinnvoll sein, einen G Data ManagementServer als **Subnet-Server** zu betreiben. Subnet-Server dienen der Entlastung des Netzwerks zwischen Clients und dem Main-MMS. Sie können in Netzwerken verwendet werden und verwalten dort die ihnen zugeordneten Clients. Die Subnet-Server bleiben funktionsfähig, auch wenn Main- oder Secondary-ManagementServer nicht erreichbar sind. Diese laden allerdings selbständig keine Virensignaturupdates.

Schematisch sähe ein **Aufbau der Server-Typen** in großen Netzwerken folgendermaßen aus: Subnet-Server bündeln die Anfragen und Meldungen einzelner Clients oder Client-Gruppen und geben sie an den Main-Server weiter. Dieser wird von einem Secondary-Server unterstützt, der die Ausfallsicherheit sicherstellt. Große Netzwerke können von der Nutzung der **Peer-to-Peer-Updateverteilung** profitieren. Durch die Aktivierung dieser Option wird die Netzauslastung zwischen Server und Client während der Updateverteilung stark reduziert. Bei einigen Netzwerken kann auf diese Weise die Installation eines Subnet-Servers überflüssig sein.



Auswahl Datenbank

Wählen Sie nun eine Datenbank aus, die der G Data ManagementServer verwenden soll. Sie haben dabei die Möglichkeit, eine vorhandene **SQL-Server-Instanz** oder **Microsoft SQL-Express** zu verwenden. Ein Server-Betriebssystem ist nicht zwingend erforderlich. Die **SQL**-Variante bietet sich vor allem in größeren Netzwerken mit einer Client-Anzahl **ab 1000** an. Die **SQL Express**-Variante bietet sich in Netzwerken mit einer Client-Anzahl **bis 1000** an.

Computername

Überprüfen Sie nun den **Namen** des Rechners, auf dem der G Data ManagementServer installiert wird. Dieser Rechner muss über den hier angegebenen Namen von den Clients im Netzwerk angesprochen werden können.

Produktaktivierung

Während der Installation erfolgt die **Produktaktivierung**. Diese ermöglicht das Laden von Updates nach Beendigung der Installation.

- **Registriernummer eingeben**: Wenn Sie die G Data Software das erste Mal installieren, wählen Sie diese Option aus und geben anschließend die Registriernummer ein, die dem Produkt beiliegt. Sie finden diese je nach Art des Produktes auf der Lizenzurkunde (MediaPack) oder in der Auftragsbestätigung. Kontaktieren Sie im Zweifelsfall Ihren Händler bzw. den betreuenden Distributor. Durch die Eingabe der Registrierungsnummer wird Ihr Produkt aktiviert. Die erstellten Zugangsdaten werden Ihnen nach erfolgreicher Registrierung angezeigt. **Notieren Sie sich unbedingt diese Zugangsdaten!** Nach erfolgter Registrierung ist eine erneute Eingabe des Lizenzschlüssels nicht mehr möglich.

  > Sollten Sie bei der Eingabe der Registriernummer Probleme haben, überprüfen Sie die Registriernummer auf die korrekte Eingabe. Je nach verwendeten Schriftsatz wird ein großes "I" (wie Ida) oft als die Ziffer "1", bzw. dem Buchstaben "l" (wie Ludwig) fehlinterpretiert. Das Gleiche gilt für: "B" und "8", "G" und 6, "Z" und "2".

- **Zugangsdaten eingeben**: Wenn die G Data Software schon einmal installiert wurde, haben Sie Zugangsdaten (**Benutzername** & **Passwort**) erhalten. Um die G Data Software erneut zu installieren, geben Sie hier die Zugangsdaten an.

- **Später aktivieren**: Wenn Sie sich zunächst nur einen Überblick über die Software verschaffen möchten oder die Zugangsdaten für den Moment nicht greifbar sind, kann die Installation auch ohne Angabe von Daten installiert werden. Da auf diese Weise allerdings vom Programm keine Aktualisierungen aus dem Internet geladen werden, ist kein echter Schutz vor Schadsoftware gegeben. Nur mit tagesaktuellen Updates kann die G Data Software Ihren Computer effektiv schützen. Eine Nutzung der Software ohne Aktivierung schützt Sie nur unzureichend. Sie können Ihre

Registrierungsnummer oder Ihre Zugangsdaten jederzeit nachträglich eingeben. Lesen Sie hierzu auch die **Hinweise zur nachträglichen Aktivierung der G Data Software**.

> Beachten Sie: wird die Software installiert, ohne sie zu aktivieren, sind nur die G Data AntiVirus-Komponenten verfügbar, selbst wenn Sie eine G Data ClientSecurity, eine G Data EndpointProtection oder andere Module erworben haben. Die zusätzlichen Komponenten werden aktiviert und sind verfügbar, sobald die Software registriert wird.

Konfiguration Datenbanktyp

Dieser Installationsschritt erfolgt nur dann, wenn Sie den G Data ManagementServer neu installieren oder auf dem Rechner noch eine **SQL-Datenbank** vorinstalliert ist. In der Regel reicht es, diese Info-Box durch Anklicken der Schließen-Schaltfläche zu schließen.

Installationsabschluss

Nach der Installation des G Data ManagementServers ist dieser einsatzbereit. Ein Neustart des Servers könnte erforderlich sein. Um Änderungen an Clienteinstellungen vorzunehmen, können Sie unter **Start > (Alle) Programme > G Data Administrator** den Eintrag **G Data Administrator** auswählen und auf diese Weise das Administrationstool für den G Data ManagementServer starten. Der G Data ManagementServer wird bei jedem System(neu)start automatisch mitgestartet.

Installation des G Data Administrators

Bei einer Installation des **G Data ManagementServers** wird automatisch auf demselben Rechner der G Data Administrator mitinstalliert. Eine nachträgliche Installation der Administratorsoftware auf dem G Data ManagementServer ist nicht erforderlich. Die Installation des G Data Administrators kann unabhängig von der Installation auf dem Server auch auf jedem Client-Rechner erfolgen. Auf diese Weise kann der G Data ManagementServer auch dezentral betreut werden.

Zur Installation des G Data Administrators auf einem Client-Rechner legen Sie die G Data-DVD in das DVD-Laufwerk des Client-Rechners und drücken Sie die Schaltfläche **Installieren**. Wählen Sie anschließend die Komponente **G Data Administrator** durch einen Klick auf die nebenstehende Schaltfläche.

Schließen Sie spätestens jetzt alle offenen Anwendungen im Windows-System, da diese sonst zu Problemen bei der Installation führen können. Nach einem Klick auf **Weiter** wird die Installation fortgesetzt; folgen Sie dann den Installationsschritten, bei denen der Installationsassistent Sie unterstützt. Nach der Installation ist unter **Start** > **(Alle) Programme** > **G Data** > **G Data Administrator** der Eintrag **G Data Administrator** anwählbar.

Installation des G Data WebAdministrators

Legen Sie die G Data-DVD ein und drücken Sie die Schaltfläche **Installieren**. Wählen Sie anschließend die Komponente **G Data WebAdministrator** durch einen Klick auf die nebenstehende Schaltfläche.

Die Installation des G Data WebAdministrators ist einfach und unkompliziert. Nachdem Sie den Lizenzbedingungen zugestimmt haben, wählen Sie den Installationsordner aus, in dem der WebAdministrator installiert werden soll. Empfohlen wird, diesen im HTTP-Verzeichnis des Webservers zu installieren (z.B. \inetpub\wwwroot).

Während der Installation muss möglicherweise - abhängig von Systemvoraussetzungen - zusätzliche Software installiert werden:

- *Microsoft Internet Information Services (IIS):* Da der WebAdministrator ein webbasiertes Produkt ist, muss der Server, auf dem es installiert wird, auch als Webserver nutzbar sein. Der WebAdministrator unterstützt Microsoft Internet Information Services (IIS). Bitte stellen Sie sicher, das IIS auf Ihrem Server läuft, bevor Sie den WebAdministrator installieren.
- *Kompatibilität mit IIS-Metabasis und IIS 6-Konfiguration*: Vor der Installation des G Data WebAdministrators ist die Aktivierung der Windows-Funktion Kompatibilität mit IIS-Metabasis und IIS 6-Konfiguration erforderlich. Sollte diese Funktion nicht zur Verfügung stehen, wird die Installation des G Data WebAdministrators abgebrochen. Sie finden diesen Eintrag z.B. bei Windows Vista unter **Start > Systemsteuerung > Programme > Programme und Funktionen > Windows-Funktionen** ein- oder ausschalten. Hier können Sie den Eintrag unter **Internetinformationsdienste > Webverwaltungstools > Kompatibilität mit der IIS 6-Verwaltung > Kompatibilität mit IIS-Metabasis und IIS 6-Konfiguration** an- oder ausschalten. Außerdem müssen - soweit nicht schon geschehen - die **WWW-Dienste** aktiviert sein. Hierzu setzen Sie das Häkchen unter **Internetinformationsdienste > WWW-Dienste**. In Serverbetriebssystemen finden sich die entsprechenden Optionen im Servermanager bei **Rollen**.
- *Microsoft .NET Framework*: Der WebAdministrator basiert auf dem .NET Framework von Microsoft. Sollte auf dem Server kein Microsoft .NET Framework installiert sein, fordert Sie der Installationsassistent des WebAdministrators dazu auf, dieses zu installieren. Nach der Installation ist ein Neustart erforderlich.
- *Microsoft Silverlight*: Der G Data WebAdministrator benötigt Microsoft Silverlight. Falls dies bei der Installation nicht vorhanden ist, werden Sie beim ersten Start des G Data WebAdministrators darauf aufmerksam gemacht.

Nach der Installation steht Ihnen auf dem Desktop Ihres Computers das Symbol für den **G Data WebAdministrator** zur Verfügung. Darüber hinaus erhalten Sie einen Hyperlink, mit dem Sie den WebAdministrator über Ihren Browser aufrufen können.

Die Verwendung des WebAdministrators übers Internet ohne eine sichere Verbindung ist ein potentielles Sicherheitsrisiko. Optimalerweise verwenden Sie bitte ein **SSL Server Zertifikat in IIS.**

Installation des G Data MobileAdministrators

Legen Sie die G Data-DVD ein und drücken Sie die Schaltfläche **Installieren**. Wählen Sie anschließend die Komponente **G Data MobileAdministrator** durch einen Klick auf die nebenstehende Schaltfläche.

Die Installation des G Data MobileAdministrators ist der des **WebAdministrators** vergleichbar. Nachdem Sie den Lizenzbedingungen zugestimmt haben, wählen Sie den Installationsordner aus, in dem der MobileAdministrator installiert werden soll. Empfohlen wird, diesen im HTTP-Verzeichnis des Webservers zu installieren (z.B. \inetpub\wwwroot).

Während der Installation muss möglicherweise - abhängig von Systemvoraussetzungen - zusätzliche Software installiert werden:

- *Microsoft Internet Information Services (IIS)*: Da der MobileAdministrator ein webbasiertes Produkt ist, muss der Server, auf dem es installiert wird, auch als Webserver nutzbar sein. Der MobileAdministrator unterstützt Microsoft Internet Information Services (IIS). Bitte stellen Sie sicher, das IIS auf Ihrem Server läuft, bevor Sie den MobileAdministrator installieren.

- *Microsoft .NET Framework*: Der MobileAdministrator basiert auf dem .NET Framework von Microsoft. Sollte auf dem Server kein Microsoft .NET Framework installiert sein, fordert Sie der Installationsassistent des MobileAdministrators dazu auf, dieses zu installieren. Nach der Installation ist ein Neustart erforderlich.

Nach Beendigung der Installation stellt Ihnen der Installer einen Direktlink für den MobileAdministrator zur Verfügung, über den Sie diesen mit Ihrem Smartphone über einen Mobile Browser erreichen und bedienen können.

Die Verwendung des MobileAdministrators übers Internet ohne eine sichere Verbindung ist ein potentielles Sicherheitsrisiko. Optimalerweise verwenden Sie bitte ein **SSL Server Zertifikat in IIS**.

Installation der G Data Security Clients

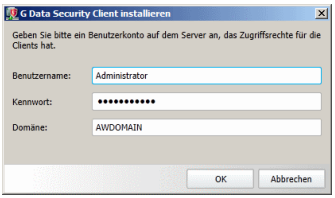
Zum Schutz und zur Verwaltung des Netzwerks sollte der G Data Security Client auf jedem Rechner im Netzwerk installiert sein. Je nach Einsatz-Szenario können Sie die Installation der Client-Software über eine **Remote-Installation** (über den G Data Administrator) oder über eine **lokale Installation** (per G Data software DVD oder ein Client-Installationspaket) durchführen. Darüber hinaus ist es auch empfehlenswert, den G Data Security Client auch auf dem Server zu installieren.

Remote-Installation

Der bequemste Weg, um die Client-Software auf den Clients zu installieren, ist die Remote-Installation über den G Data Administrator. Über den **Server-Einrichtungsassistent** können Sie automatisch den G Data Security Client auf allen im Netzwerk angeschlossenen Rechnern installieren.

Abgesehen von den erforderlichen **Port-Konfigurationen** sind folgende Voraussetzungen nötig, um eine Remote-Installation durchzuführen.:

- Sofern eine Firewall verwendet wird, muss für die Datei gdmms.exe eine Ausnahme definiert sein.
- In einer Windows-Arbeitsgruppe muss unter Windows XP die einfache Dateifreigabe, unter Windows Vista bzw. Windows 7 die Option Freigabeassistent verwenden deaktiviert werden. Zusätzlich sollte die Benutzerkontensteuerung (UAC) deaktiviert sein.
- Ein Zugriff auf die Freigaben C$ und Admin$ des Clients ist erforderlich.
- Es muss ein Passwort vergeben sein. Ein leeres Passwort ist nicht zulässig.
- In den **Diensten** muss der Remoteregistrierungsdienst aktiv sein.



Über den **Server-Einrichtungsassistenten**, der automatisch beim ersten Start des G Data Administrator aufgerufen wird, erhalten Sie einen Überblick über alle in Ihrem Netzwerk angemeldeten Computer. Darüber hinaus können Sie manuell weitere Computer per Namenseingabe hinzufügen und aktivieren. Nun können Sie den G Data Security Client einfach dadurch auf diesen Rechnern installieren, indem Sie einen Rechtsklick durchführen und in dem erscheinenden Kontextmenü **G Data Security Client installieren** auswählen. Nun erscheint ein Eingabefenster, in dem Sie **Benutzername**, **Kennwort** und **Domäne** mit Zugriffsrechten auf den Clients eingeben können. Nach Auswahl der Anzeigesprache werden Sie gefragt, ob Sie mit dem Client zugleich die G Data Firewall auf dem jeweiligen Client mit installieren möchten. Die Firewall steht Ihnen nur bei den **Software-Versionen** G Data ClientSecurity, G Data EndpointProtection, and G Data SmallBusiness Security zur Verfügung. Ein Dialogfenster zeigt Ihnen den Verlauf des Installationsprozesses. Nach einer erfolgreichen Installation der Software muss der Client-Rechner neu gestartet werden.

> Wenn Sie die **Active Directory Integration** nutzen, können Sie die Client-Software auch automatisch auf neu ins Netzwerk eingebundene Rechner installieren.

Die Remote-Installation kann auf zwei verschiedene Arten erfolgen. Wenn der Client die notwendigen Voraussetzungen erfüllt, können die Installationsdaten direkt vom Server aus überspielt und entsprechende Änderungen in der Registry vorgenommen werden. Wenn der Server nur Zugriff auf die Festplatte des Client-Rechners und nicht auf die Registry hat oder andere Systemvoraussetzungen nicht erfüllt sind, dann wird das Setup-Programm auf den Client kopiert und die Installation wird automatisch beim nächsten Neustart des Computers gestartet.

Wenn die Client-Software nicht über die Remote-Installation installiert werden kann, haben Sie darüber hinaus die Möglichkeit, die Client-Software lokal über die G Data Software DVD oder das Client-Installationspaket durchzuführen. Ein Client-Installationspaket kann auch über **logon scripts/group policy objects** verteilt werden.

Lokale Installation

Wenn eine **Remote-Installation** nicht möglich ist, können Sie den G Data Security Client auch direkt manuell auf den Clients installieren. Sie können die G Data Software DVD dazu verwenden, entweder die Client-Software direkt auf dem Client zu installieren oder ein Installationspaket zu erzeugen, welches dann die Installation im Hintergrund durchführt (ideal für die Distribution der Software über Login-Skripts).

G Data Software DVD

Zur lokalen Installation des Clients auf einem Client-Rechner legen Sie die G Data-DVD in das DVD-Laufwerk des Client-Rechners ein und drücken Sie die Schaltfläche **Installieren**. Wählen Sie anschließend die Komponente **G Data Security Client** durch einen Klick auf die nebenstehende Schaltfläche.

Geben Sie im Verlauf der Installation den **Servernamen** oder die **IP-Adresse des Servers** ein, auf dem der G Data ManagementServer installiert ist. Die Angabe des Servernamens ist notwendig, damit der Client über das Netzwerk mit dem Server in Kontakt treten kann.

Client Installationspaket

Das Paket ist eine einzelne ausführbare Datei (GDClientPck.exe), mit der ein neuer Client ohne weitere Benutzerinteraktion auf einem zu schützenden Rechner installiert werden kann. Das Installationspaket eignet sich beispielsweise dazu, den Client via Login-Script auf allen Rechnern einer Domäne zu verteilen oder dieses direkt lokal zu installieren. Das Paket enthält immer die auf dem Server aktuelle Client-Version.

Um ein Installationspaket zu erstellen, starten Sie den G Data Administrator. Im Menü **Organisation** wählen Sie bitte die Option **G Data Security Client Installationspaket erstellen**. Nun werden Sie aufgefordert, den ManagementServer auszuwählen, an welchem der Client sich registrieren soll und die Installationssprache. Nach der Auswahl eines Speicherortes erstellt der G Data Administrator nun ein Installationspaket im Hintergrund. Es ist unbedingt erforderlich, das Installationspaket auf den Zielrechner zu kopieren und dort mit Administrator-Rechten zu starten. Nun wird der G Data Security Client ohne weitere Benutzerinteraktion installiert.

Installation von Linux-Clients

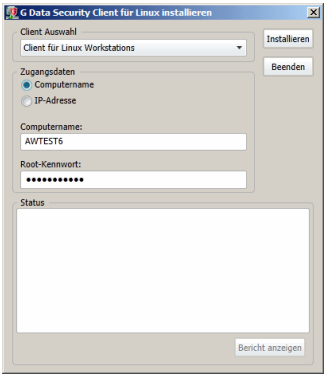
Der Linux-Client kann (ebenso wie die Windows-Clients) in die Infrastruktur des G Data ManagementServers eingebunden und zentral über die G Data Administrator-Software gesteuert und mit Signaturupdates versorgt werden. Analog zu den Windows-Clients wird auch bei Linux-Clients ein Dateisystemwächter mit einer grafischen Benutzeroberfläche eingerichtet, die sich in der Funktionalität an der Windows-Version orientiert. Für Linux-Rechner, die als Fileserver arbeiten und verschiedenen Clients Windows-Freigaben (über das SMB-Protokoll) zur Verfügung stellen, kann hierzu ein Modul installiert werden, das den Zugriff auf die Freigaben kontrolliert und bei jedem Zugriff einen Scan auf die Datei ausführt, so dass keine Malware vom Samba-Server auf die Windows-Clients (und umgekehrt) gelangen kann.

> Für den Workstation-Client ist eine Kernel-Version größer gleich 2.6.25 erforderlich, dies ist z.B. bei Ubuntu 8.10, Debian 5.0, Suse Linux Enterprise Desktop 11 und anderen aktuellen Distributionen der Fall. Bei anderen Distributionen ist im Einzelfall eine Anpassung erforderlich. Der Fileserver-Client lässt sich auf allen gängigen Distributionen verwenden.

Remote-Installation

Um die Software auf dem Linux-Client zu installieren, gehen Sie folgendermaßen vor:

1. Wählen Sie im Aufgabenbereich **Clients** im Menü **Clients** den Befehl **G Data Client für Linux installieren** aus. Nun erscheint ein Dialogfenster über das Sie den Client definieren können, auf den die Client-Software kopiert werden soll. Der Rechner muss dazu im Netzwerk bekannt sein.
2. Verwenden Sie die Auswahl **Computername**, wenn auf dem Client-Rechner ein Samba-Dienst installiert ist oder wenn der Rechner im Nameserver des Netzwerkes registriert ist. Sollte der Name des Rechners nicht bekannt sein, verwenden Sie die **IP-Adresse** des Rechners.
3. Geben Sie nun das **Root-Kennwort** des Rechners ein. Für eine Remote-Installation muss ein Root-Kennwort vergeben sein. Standardmäßig ist dies unter einigen Distributionen (z.B.) Ubuntu nicht der Fall.
4. Drücken Sie nun auf die **Installieren**-Schaltfläche. Im Bereich **Status** sehen Sie, ob die Installation erfolgreich war.



Lokale Installation

Im Verzeichnis **\Setup\LinuxClient** auf der G Data-DVD finden Sie die folgende Dateien

- **installer.bin** (Installer für den Linux-Client)
- **uninstaller.sh** (Uninstaller für den Linux-Client)

Sie können diese Dateien auf den Client-Rechner kopieren und zur Installation der Client-Software die entsprechende Datei starten. Zusätzlich finden Sie auf der G Data-DVD noch eine Datei mit den Virensignaturen. Da die Software nach der Installation aber automatisch die neuesten Virensignaturen vom Server bezieht, ist die Installation dieser Datei fakultativ:

- **signatures.tar** (Archiv mit Virensignaturen)

Installation der G Data MailSecurity

Vor der Installation sollten Sie sich Gedanken darüber machen, wo im Netzwerk Sie G Data MailSecurity installieren. Während Sie die G Data MailSecurity-Administratorsoftware von jedem Punkt des Netzwerks aus verwenden können, benötigt die Installation des eigentlichen MailGateways einiger Vorüberlegungen. Generell sollte sich das MailGateway am besten direkt hinter Ihrer Netzwerk-Firewall befinden (soweit vorhanden), d.h. dass der SMTP/POP3-Datenstrom aus dem Internet über die Firewall direkt zum MailGateway geleitet und von dort weiter verteilt wird.

> Bitte beachten Sie, dass Sie gegebenenfalls Ihre Firewall-Konfigurationen (IP-Adresse und/oder Port) verändern müssen, damit der E-Mailverkehr über das G Data MailSecurity MailGateway abgewickelt wird.

Prinzipiell können Sie das G Data MailSecurity MailGateway auf einem eigenen Rechner installieren, der dann für das gesamte Netzwerk als MailGateway fungiert, es ist aber auch möglich, G Data MailSecurity auf dem Rechner einzusetzen, der gleichzeitig als Mail-Server dient. Dabei ist zu beachten, dass eine gemeinsame Installation auf einem einzigen Rechner bei starkem Mail-Aufkommen zu Verzögerungen führen kann, da sowohl die Verwaltung permanenter E-Mail-Kommunikation, als auch die immanenten Virenanalyse sehr rechenintensive Vorgänge sind.

Installation des MailGateways auf dem Mail-Server (SMTP)

Wenn Ihr SMTP-Server die Änderung der Port-Nummer erlaubt, können Sie G Data MailSecurity auch auf demselben Rechner installieren, wie Ihren SMTP-Server. In diesem Fall vergeben Sie bitte für Ihren Original-Mail-Server einen neue Port-Nummer (z.B. 7100 oder höher). Das MailGateway verwendet dann weiterhin Port 25 zur Verarbeitung eingehender Mails.

Sollten Sie G Data MailSecurity auf demselben Rechner wie Microsoft Exchange 5.5 installieren, kann das G Data MailSecurity Setup automatisch den Port für eingehende Mails umstellen. Dazu wird der SMTP-Eintrag in der Datei *\winnt\system32\drivers\etc\services* verändert und der Internet Mail Dienst von Microsoft Exchange neu gestartet.

Konfigurations-Beispiel

Konfiguration Mail-Server

- Port für eingehende Mails: 7100 (Beispiel)
- Nachrichtenübermittlung: Alle Nachrichten zum Host weiterleiten: 127.0.0.1

Konfiguration G Data MailSecurity MailGateway (Eingehended (SMTP))

- Port, auf dem die Mails eingehen: 25
- DNS zum Versenden der Mails verwenden: AUS
- Mails an diesen SMTP-Server weiterleiten: 127.0.0.1

- Port: 7100 (Beispiel)

Konfiguration G Data MailSecurity MailGateway (Ausgehend (SMTP))

- Ausgehende Mail verarbeiten: EIN
- IP-Adressen der Server, die ausgehende Mails senden können: 127.0.0.1;<IP Mail-Server>
- DNS zum Versenden der Mails verwenden: EIN

Installation des MailGateways auf separatem Rechner (SMTP)

Hierbei müssen eingehende Mails an das G Data MailSecurity MailGateway gesendet werden (nicht an den Mail-Server). Das kann über unterschiedliche Methoden erreicht werden:

a) den MX-Record im DNS-Eintrag anpassen

b) Umleitung an der Firewall definieren (falls vorhanden)

c) die IP-Adresse des Mail-Servers ändern und dem Rechner mit dem G Data MailSecurity MailGateway die originale IP-Adresse des Mail-Servers zuweisen

Konfiguration

Konfiguration Mail-Server

- Port für eingehende Mails: 25
- Nachrichtenübermittlung: Alle Nachrichten zum Host weiterleiten: <IP G Data MailSecurity MailGateway>

Konfiguration G Data MailSecurity MailGateway (Eingehend (SMTP))

- Port, auf dem die Mails eingehen: 25
- DNS zum Versenden der Mails verwenden: AUS
- Mails an diesen SMTP-Server weiterleiten: <IP Mail-Server>
- Port: 25

Konfiguration G Data MailSecurity MailGateway (Ausgehend (SMTP))

- Ausgehende Mail verarbeiten: EIN
- IP-Adressen der Server, die ausgehende Mails senden können: <IP Mail-Server>
- DNS zum Versenden der Mails verwenden: EIN

Installationsvorgang

Schließen Sie bitte alle anderen Programme, bevor Sie mit der Installation von G Data MailSecurity beginnen. Es kann zu Fehlfunktionen oder einem Abbruch kommen, falls z.B. Programme geöffnet sind, die auf Daten zugreifen, die G Data MailSecurity zur Installation benötigt. Beachten Sie bitte auch, dass für eine Installation ausreichender Festplattenspeicherplatz auf Ihrem System zur Verfügung steht. Sollte während der Installation nicht genügend Speicherplatz zur Verfügung stehen, weist Sie das Installationsprogramm von G Data MailSecurity darauf hin. Die Installation von G Data MailSecurity ist ausgesprochen unkompliziert. Starten Sie einfach Ihr Windows und legen dann die G Data MailSecurity-CD-ROM in Ihr CD-ROM-Laufwerk ein. Es öffnet sich automatisch ein Installationsfenster, welches Ihnen folgende Optionen bietet:

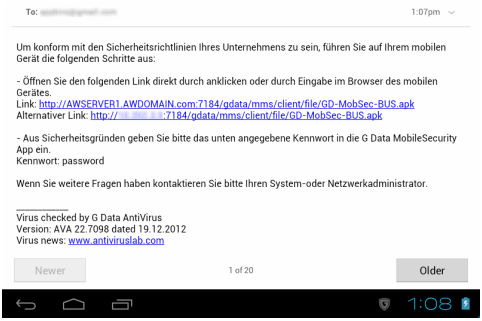
- **Installieren**: Hiermit starten Sie die Installation von G Data MailSecurity auf Ihrem Computer.
- **Durchsuchen**: Über den Windows-Explorer können Sie hier die Verzeichnisse der G Data MailSecurity-CD-ROM sichten.
- **Abbrechen**: Über diesen Eintrag können Sie die den Autostart-Bildschirm schließen, ohne eine Aktion durchzuführen.

Folgen Sie nun einfach den einzelnen Schritten des Installationsassistenten und installieren Sie über die Schaltfläche **G Data MailSecurity** das MailGateway auf dem Rechner, den Sie dafür verwenden möchten. Das kann im besten Fall ein speziell dafür abgestellter MailGateway-Rechner sein, aber auch der Mail-Server-Rechner selber bzw. irgendein anderer Computer, der im Netzwerk administrative Aufgaben übernehmen kann. Bitte beachten Sie in diesem Zusammenhang die **Mindestsystemvoraussetzungen**, die für den Betrieb des MailGateways notwendig sind.

> Wenn Sie die Komponenten für die statistische Auswertung installieren, hat der G Data MailSecurity Administrator im Status-Bereich eine Statistik-Schaltfläche. Hierüber können Sie sich statistische Informationen über den Mailserver anzeigen lassen. Wie die Anzeige dieser Statistik konfiguriert werden kann, lesen Sie im Kapitel: **Optionen > Logging**.

Installation der G Data MobileSecurity

Um von den Möglichkeiten des G Data Mobile Device Management Gebrauch zu machen, können Sie eine auf Business-Belange ausgelegte Spezialversion der G Data MobileSecurity auf Ihren Android-Geräten installieren. Der G Data Administrator bietet dabei Installationsmöglichkeiten für mobile Clients im **Clientauswahlbereich**. Klicken Sie auf die Schaltfläche **Installationslink an mobile Clients senden**, um eine Mail an die betreffenden Android-Geräte zu versenden. In dieser Mail befindet sich ein Download-Link für die MobileSecurity App. Sie können den Versand direkt an mehrere Mail-Adressen durchführen, in dem Sie diese - getrennt durch Zeilenumbruch oder Komma - eingeben. Wenn Sie bis jetzt noch kein Passwort eingegeben haben, können Sie es im Bereich **Einstellungen** unter **Authentifizierung für mobile Clients** nachholen.


To:
1:07pm
Um konform mit den Sicherheitsrichtlinien Ihres Unternehmens zu sein, führen Sie auf Ihrem mobilen Gerät die folgenden Schritte aus:
- Öffnen Sie den folgenden Link direkt durch anklicken oder durch Eingabe im Browser des mobilen Gerätes.
Link: http://AWSERVER1.AWDOMAIN.com:7184/gdata/mms/client/file/GD-MobSec-BUS.apk
Alternativer Link: http://:7184/gdata/mms/client/file/GD-MobSec-BUS.apk
- Aus Sicherheitsgründen geben Sie bitte das unten angegebene Kennwort in die G Data MobileSecurity App ein.
Kennwort: password
Wenn Sie weitere Fragen haben kontaktieren Sie bitte Ihren System-oder Netzwerkadministrator.
Virus checked by G Data AntiVirus
Version: AVA 22.7098 dated 19.12.2012
Virus news: www.antiviruslab.com
Newer
1 of 20
Older
1:08

Nach dem Versand können Sie oder Ihre Mitarbeiter die Mail auf dem mobilen Gerät öffnen und durch Antippen des Download-Links die APK-Datei installieren. Bitte beachten Sie, dass die Option **Unbekannte Quellen (Installation von Nicht-Market Apps erlauben)** aktiviert sein muss, damit die Datei installiert werden kann. Diese Option finden Sie normalerweise im Android-System-Menü unter **Einstellungen > Sicherheit > Geräteverwaltung**.

Nach dem Öffnen der APK-Datei und dem Bestätigen der benötigten Berechtigungen wird die G Data MobileSecurity installiert und kann aus dem Android-App-Menü heraus gestartet werden. Über die Einstellungen-Schaltfläche oben rechts im Programmbildschirm können Sie nun die Remote-Administration erlauben. Wählen Sie hierzu den Eintrag **Remote-Administration erlauben** aus und und geben Sie den Namen oder die IP-Adresse des ManagementServers unter **Server-Adresse** ein. Unter **Gerätename** können Sie nun für das Android-Gerät einen Namen zuweisen, unter dem dieses im G Data Administrator ermittelt werden kann. Bei **Passwort** sollten Sie das Passowrt eintragen, welches Sie auch beim G Data Administrator eingetragen haben (dieses Passwort ist auch in der Mail angegeben, die Ihnen mit dem Download-Link ans Android-Gerät geschickt wurde).

Das Gerät wird nun neben den anderen Clients im **Clients**-Bereich des G Data Administrators angezeigt und kann von dort aus administriert werden. Sollte das Gerät nicht automatisch in dieser Liste erscheinen, rebooten Sie bitte das Gerät, um das Einchecken beim G Data ManagementServer zu forcieren.

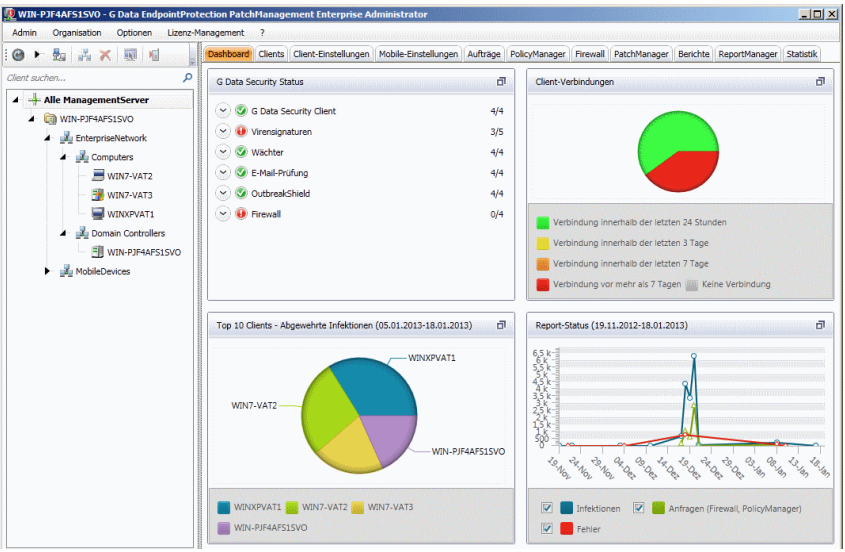
G Data ManagementServer

Der G Data ManagementServer ist das Herzstück der G Data Architektur: Er verwaltet die Clients, fordert neueste Software- und Virensignaturupdates automatisch vom G Data UpdateServer an und steuert den Virenschutz im Netzwerk. Zur Kommunikation mit den Clients nutzt der G Data ManagementServer das TCP/IP-Protokoll. Für Clients, die vorrübergehend keine Verbindung zum G Data ManagementServer haben, werden die Jobs automatisch gesammelt und beim nächsten Kontakt zwischen G Data Security Client und G Data ManagementServer synchronisiert. Der G Data ManagementServer verfügt über einen zentralen Quarantäne-Ordner. In diesem können verdächtige Dateien verschlüsselt sichergestellt, gelöscht, desinfiziert oder gegebenenfalls an die Internet-Ambulanz weitergeleitet werden. Der G Data ManagementServer wird über den **G Data Administrator** gesteuert.

> Wenn Sie den G Data Administrator beenden, bleibt der G Data ManagementServer weiterhin im Hintergrund aktiv und steuert die Prozesse, die von Ihnen für die Clients eingestellt wurden.

G Data Administrator

Der G Data Administrator ist die Steuerungssoftware für den G Data ManagementServer, die die Verwaltung von Einstellungen und Updates für alle im Netzwerk installierten G Data-Clients ermöglicht. Der G Data Administrator ist passwortgeschützt und kann auf jedem Windows-Rechner innerhalb des Netzwerkes installiert und gestartet werden. Im G Data Administrator lassen sich Scanaufträge und Wächterfunktionen sowie Änderungen von Einstellungen vornehmen. Automatische Clientinstallationen, Software- und Virensignaturupdates, werden ebenfalls dort festgelegt.



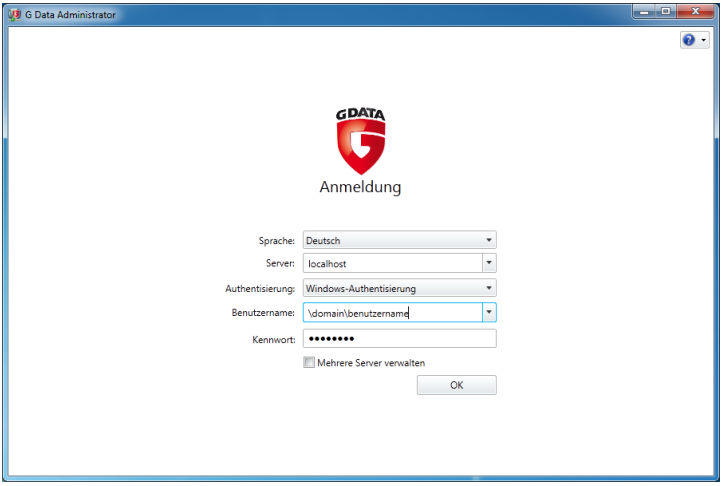
Die Oberfläche des G Data Administrators ist in folgende Bereiche untergliedert:

- Der links befindliche **Clientauswahlbereich** zeigt alle Clients, die bereits aktiviert sind und auf welchen die G Data Client Software schon installiert ist oder installiert werden kann.
- Rechts davon kann über Karteireiter in die jeweiligen **Aufgabenbereiche** gewechselt werden. Der Inhalt des Aufgabenbereiches bezieht sich normalerweise auf den im Clientauswahlbereich markierten Computer bzw. auf die markierte Gruppe von Clients.
- Oberhalb dieser Spalten finden Sie eine Menüleiste für globale Funktionen, die in allen Aufgabenbereichen verwendet werden können, sowie Sonderfunktionen für ausgewählte Aufgabenbereiche.

Bei der Administration von Linux-Clients, die auf Samba-Servern installiert sind, sind Funktionen, die z.B. den Umgang mit E-Mails beinhalten, gesperrt, da diese im Kontext eines Fileservers nicht notwendig sind. Funktionen, die für Linux-Clients nicht einstellbar sind, werden durch ein rotes Ausrufezeichen vor der jeweiligen Funktion markiert.

Starten des G Data Administrators

Das Administrator-Tool zur Steuerung des G Data ManagementServers wird mit einem Klick auf den Eintrag **G Data Administrator** in der Programmgruppe **Start** > **(Alle) Programme** > **G Data** > **G Data Administrator** des Startmenüs aufgerufen.



Beim Starten des G Data Administrators werden Sie nach dem **Server**, **Authentisierung**, **Benutzername** und **Kennwort** gefragt. Geben Sie in dem Feld **Server**, den Namen des Computers ein, auf dem der G Data ManagementServer installiert wurde. Wählen Sie nun Ihre **Authentisierung** aus.

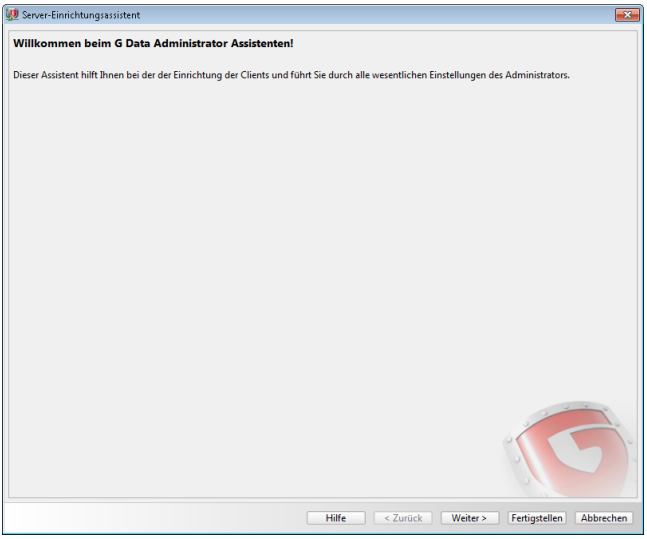
- **Windows-Authentisierung**: Wenn Sie diese Authentisierungsvariante wählen, können Sie sich mit dem Benutzernamen und Passwort Ihres Windows-Administrator-Zugangs auf dem G Data ManagementServer einloggen.
- **SQL-integrierte Authentisierung**: Wenn Sie einen existierenden SQL-Server nutzen möchten, wählen Sie diese Option und loggen sich mit Ihren SQL-Server-Anmeldeinformationen ein.
- **Integrierte Authentisierung**: Wenn Sie weder die Windows-, noch die SQL-Server-Authentisierung nutzen möchten, können Sie sich auch über ein im G Data ManagementServer integriertes Authentisierungssystem einloggen. Weitere Accounts können über die Funktion **Benutzerverwaltung** angelegt werden.

G Data Administrator konfigurieren

Administrative Einstellungen

Server-Einrichtungsassistent

Mit dem Einrichtungsassistenten lassen sich im Netzwerk die Clients auswählen und aktivieren, für die die G Data Software den Virenschutz bereitstellen soll. Der Einrichtungsassistent wird automatisch beim ersten Starten des G Data Administrators ausgeführt, kann aber auch nachträglich jederzeit über das **Admin**-Menü erneut durchgeführt werden.


Server-Einrichtungsassistent
Willkommen beim G Data Administrator Assistenten!
Dieser Assistent hilft Ihnen bei der der Einrichtung der Clients und führt Sie durch alle wesentlichen Einstellungen des Administrators.
Hilfe
< Zurück
Weiter >
Fertigstellen
Abbrechen

Aktivieren

Zunächst müssen alle Clients, die von der G Data Software überwacht werden sollen, aktiviert werden. Die zu aktivierenden Clients müssen zunächst markiert und mit einem Klick auf **Aktivieren** aktiviert werden. Eventuell sind einige Computer nicht in der Liste enthalten (z.B. weil die betreffenden Rechner lange nicht eingeschaltet waren oder keine Datei- bzw. Druckerfreigabe eingerichtet haben). Zum Aktivieren dieser Clients wird im Eingabefeld **Computer** der Name des Rechners eingegeben. Nach einem Klick auf **Aktivieren** wird der zu aktivierende Rechner in die Clientliste aufgenommen. Wenn alle zu schützenden Rechner aktiviert wurden, folgt nach einem Klick auf **Weiter** der nächste Schritt.

Installieren

Im folgenden Dialog ist das Häkchen bei **Client-Software automatisch auf den aktivierten Computern installieren** voreingestellt. Wenn die Verteilung der Software auf den Client-Rechnern zu einem späteren Zeitpunkt erfolgen soll, muss diese Option durch Entfernen des Häkchens deaktiviert werden.

Internet-Update

Der G Data ManagementServer lädt über das Internet neue Virensignaturen und Programmdateien herunter. Damit dieser Vorgang automatisch erfolgen kann, ist die Eingabe der **Zugangsdaten** erforderlich, die bei der Online-Registrierung erstellt wurden. Eine detaillierte Beschreibung zur Planung von Updateintervallen finden Sie im Kapitel **Internet-Update**. Es besteht auch die Möglichkeit, das Internet-Update nachträglich über die G Data Administrator-Programmoberfläche zu automatisieren.

E-Mail-Benachrichtigung

Im Fall eines Virenfundes auf einem oder mehreren Clients oder bei anderen kritischen Situationen kann der Netzwerkadministrator per Mail informiert werden. Geben Sie dazu die E-Mail-Adresse des Empfängers der Warnmeldungen an. Über die **Begrenzung** lässt sich ein übermäßiges Mailaufkommen im Fall eines massiven Virenbefalls verhindern. Mit **Fertigstellen** wird der Assistent beendet.

Automatische Installation der Client-Software

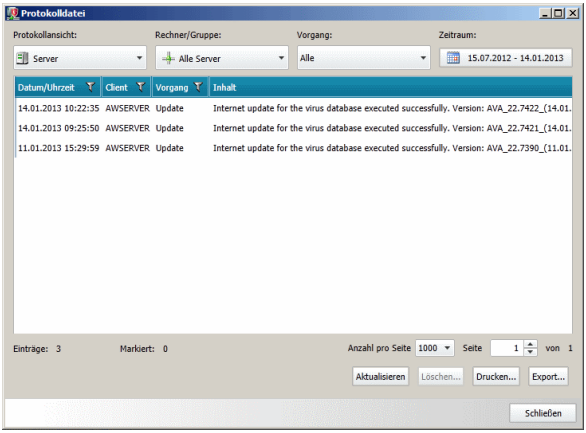
Wenn Sie die Option **Client-Software automatisch auf den aktivierten Computern installieren** auswählen, führt der Einrichtungsassistent eine **Remote-Installation** des G Data Security Client auf allen ausgewählten Netzwerk-Geräten durch.

Protokoll anzeigen

In der Protokolldatei steht ein Überblick über die letzten von der G Data Software durchgeführten Aktionen zur Verfügung. Hier werden sämtliche relevanten Informationen angezeigt. Die Anzeige des Protokolls kann nach folgenden Kriterien gefiltert werden:

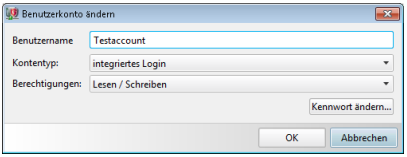
- **Protokollansicht**: Legen Sie hier fest, ob Sie ein Protokoll von den Client- oder Servervorgängen einsehen möchten.
- **Rechner/Gruppe**: Hier können Sie festlegen, ob Sie sich ein Protokoll aller Clients bzw. Gruppen oder nur einzelner Bereiche anschauen möchten.
- **Vorgang**: Definieren Sie hier, ob Sie alle protokollierten Informationen einsehen möchten oder nur Meldungen zu bestimmten Themen.
- **Zeitraum**: Hier können Sie den von/bis Zeitraum definieren, für den Protokollinformationen eingesehen werden sollen.

Das Feld **Aktualisieren** dient dazu, Vorgänge mit aufzulisten, die sich ereignen, während die Protokollansicht geöffnet ist. Sämtliche Vorgänge erscheinen erst einmal in chronologischer Reihenfolge und lassen sich durch einfaches Klicken auf die jeweilige Spaltenbezeichnung nach bestimmten Kriterien sortieren. Die Spalte, nach der die aktuelle Sortierung erfolgt, wird dabei durch ein kleines Pfeilsymbol gekennzeichnet.



Benutzerverwaltung

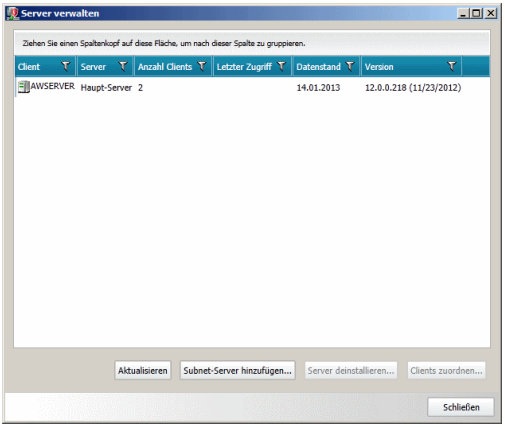
Als Systemadministrator können Sie weitere Benutzerzugänge für das G Data Administrator-Interface vergeben. Klicken Sie dazu auf die **Neu**-Schaltfläche und geben anschließend den Benutzernamen, die **Berechtigungen** dieses Nutzers (**Lesen**, **Lesen/Schreiben**, **Lesen/Schreiben/Backups wiederherstellen**) ein, definieren Sie den **Kontentyp** (**integriertes Login**, **Windows-Benutzer**, **Windows-Benutzergruppe**) und vergeben Sie ein **Kennwort** für diesen Benutzer.



Server verwalten

Über die Server-Verwaltung können Sie Clients einzelnen Subnet-Servern zuordnen, die dann die Kommunikation dieser Clients mit dem Main-Server bündeln und auf diese Weise die Netzwerknutzung optimieren. Über dieses Menü können Sie Subnet-Server installieren. Über die Schaltfläche **Clients zuordnen** können Sie vorhandene Clients den definierten Subnet-Servern zuordnen.

> Die Zuordnung der Clients zu Subnet-Servern ist unabhängig von der Gruppierung von Clients. Daher können Clients, die unterschiedlichen Subnet-Servern zugeordnet sind, dennoch in Gruppen unterteilt werden.



Subnet-Server-Synchronisation

Um eventuelle Änderungen auch außerhalb des regulären Kommunikationsintervalls von Server und Subnet-Server zu ermöglichen, kann die Subnet-Server-Synchronisation auch manuell angestoßen werden.

Beenden

Über diese Funktion wird der G Data Administrator geschlossen. Der G Data ManagementServer bleibt weiterhin gestartet und steuert den Virenschutz im Netzwerk gemäß der festgelegten Vorgaben.

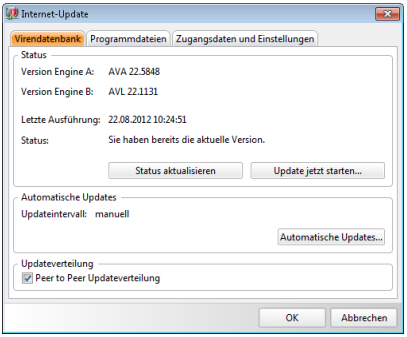
Optionen

Internet-Update

Hier werden alle Einstellungen für Internet-Updates der Virendatenbanken und der Programmdateien der G Data Software festgelegt. In der Karteikarte **Zugangsdaten und Einstellungen** sind die Zugangsdaten einzugeben, die bei der Online-Registrierung erstellt wurden. Beim Internet-Update werden die aktuellen Virendefinitionen vom G Data UpdateServer geladen und auf dem G Data ManagementServer gespeichert. Die Verteilung der Virensignaturen an die Clients wird vom Aufgabenbereich **Clients** gesteuert. Das Internet-Update stellt sicher, dass immer die aktuellen Virensignaturen und die neuesten Programmdateien vorhanden sind.

Virendatenbank

Alle Clients haben eine eigene, lokale Kopie der Virendatenbank, damit der Virenschutz auch gewährleistet ist, wenn sie offline sind (d.h. keine Verbindung mit dem G Data ManagementServer bzw. dem Internet besteht). Die **Aktualisierung** der Dateien auf den Clients erfolgt in zwei Schritten, die natürlich beide automatisiert werden können. Im ersten Schritt werden die aktuellen Dateien vom G Data UpdateServer in einen Ordner auf dem G Data ManagementServer kopiert. Im zweiten Schritt werden die neuen Dateien an die Clients verteilt (siehe Aufgabebereich **Client-Einstellungen**).



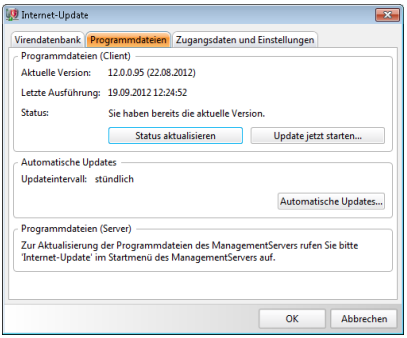
- **Status aktualisieren**: Über diese Schaltfläche können Sie die Statusanzeige der Virensignaturen gegebenenfalls aktualisieren, falls Änderungen in der Anzeige noch nicht übernommen worden sind.
- **Update jetzt starten**: Über die Schaltfläche **Update jetzt starten** können Sie eine Aktualisierung der Virendatenbanken direkt durchführen. Dabei werden die aktuellen Virensignaturen heruntergeladen, die hinterher vom G Data ManagementServer an die Clients verteilt werden.
- **Automatische Updates**: Wie die Virenprüfungen können Sie auch die Internet-Updates automatisch durchführen lassen. Aktivieren Sie dazu das Häkchen bei **Update periodisch ausführen** und legen Sie fest, wann bzw. in welchem Turnus das Update zu erfolgen hat. Damit das Update automatisch erfolgen kann, muss Ihr G Data ManagementServer mit dem Internet verbunden sein oder Sie der G Data Software eine automatische Einwahl ermöglichen. Geben Sie hierzu unter **Zugangsdaten und Einstellungen** gegebenenfalls **Benutzerkonto** und **Proxy-Einstellungen** vor.
- **Updateverteilung**: Die Verteilung kann zentral (MMS, SubnetServer > Clients) oder - wenn Sie das entsprechende Häkchenfeld aktivieren - auch dezentral (Peer to Peer) (MMS, SubnetServer, schon upgedatete Clients > Clients) erfolgen. Bitte achten Sie darauf, dass für die Updateverteilung ggf. die **Port-Konfiguration** angepasst werden muss.

Programmdateien (Client)

Wenn ein Programmupdate für die Client-Software von G Data bereit steht, können Sie die Aktualisierung der Clients über den G Data ManagementServer automatisch erledigen lassen. Die **Aktualisierung** der Dateien auf den Clients erfolgt in zwei Schritten, die beide automatisiert werden können. Im ersten Schritt werden die aktuellen Dateien vom G Data UpdateServer in einen Ordner auf dem G Data ManagementServer kopiert. Im zweiten Schritt werden die neuen Dateien an die Clients verteilt und damit wird der dortige Client aktualisiert (siehe Aufgabebereich **Client-Einstellungen**).

- **Status aktualisieren**: Über die Schaltfläche **Aktualisieren** können Sie die Statusanzeige der Softwareversion gegebenenfalls aktualisieren, falls Änderungen in der Anzeige noch nicht übernommen worden sind.
- **Update jetzt starten**: Über die Schaltfläche **Update jetzt durchführen** können Sie eine Aktualisierung der Client-Software direkt durchführen. Dabei werden die aktuellen Clientdateien heruntergeladen, die hinterher vom G Data ManagementServer an die Clients verteilt werden.
- **Automatische Updates**: Wie die Virenprüfungen können Sie auch die Internet-Updates der Client-Software automatisch durchführen lassen. Aktivieren Sie dazu das Häkchen bei **Update periodisch ausführen** und legen Sie fest, wann bzw. in welchem Turnus das Update zu erfolgen hat. Damit das Update automatisch erfolgen kann, muss der G Data ManagementServer mit dem Internet verbunden sein oder Sie der G Data Software eine automatische Einwahl ermöglichen. Geben Sie hierzu unter **Zugangsdaten und Einstellungen** gegebenenfalls **Benutzerkonto** und **Proxy-Einstellungen** vor.

  Um die Programmdateien des G Data ManagementServers zu aktualisieren, rufen Sie in der Programmgruppe **G Data ManagementServer** im Startmenü den Eintrag **Internet-Update** auf. Der G Data ManagementServer kann ausschließlich über diesen Eintrag aktualisiert werden. Dagegen kann die G Data Client-Software auch über den G Data Administrator aktualisiert werden.

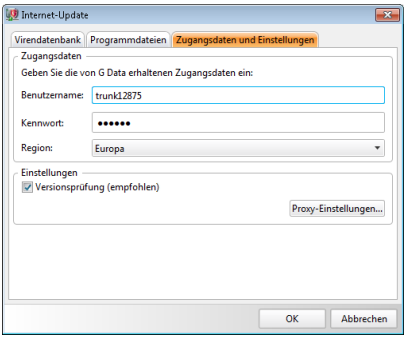


Zugangsdaten und Einstellungen

Mit der Online-Registrierung erhalten Sie von G Data die Zugangsdaten für das Update der Virendatenbanken und Programmdateien. Geben Sie diese unter **Benutzername** und **Kennwort** ein. Die (standardmäßig aktivierte) **Versionsprüfung** sollte im Regelfall immer eingeschaltet sein, da sie den Download unnötig großer Updates verhindert. Sollten sich jedoch Probleme mit Virendatenbanken einstellen, dann schalten Sie Versionsprüfung aus. Auf diese Weise wird beim nächsten Internet-Update automatisch die aktuelle Version der Virendatenbank auf den Server überspielt.

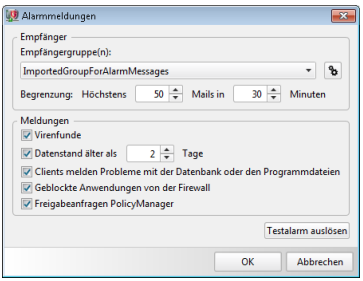
Mit der Schaltfläche **Proxy-Einstellungen** öffnen Sie ein Fenster, in dem Sie Zugangsdaten für Internet & Netzwerk eingeben können. Sie sollten hier nur Eingaben tätigen, wenn sich mit den Standardeinstellungen der G Data Software Probleme ergeben sollten (z.B. wegen der Verwendung eines **Proxyservers**) und ein Internet-Update nicht durchführbar ist.

> Die G Data Software kann die Verbindungsdaten des Internet Explorer (ab Version 4) verwenden. Konfigurieren Sie zunächst den Internet Explorer und prüfen Sie, ob die Testseite unseres Update-Servers erreichbar ist: *http://ieupdate.gdata.de/test.htm*. Schalten Sie anschließend die Option **Proxyserver verwenden** aus. Geben Sie unter **Benutzerkonto** das Konto ein, für den Sie den Internet Explorer konfiguriert haben (als das Konto, mit dem Sie sich an Ihrem Rechner angemeldet haben).



Alarmmeldungen

Bei neuen Virenfunden kann der G Data ManagementServer automatisch Alarmmeldungen per E-Mail versenden. Die dazu benötigten Einstellungen werden in diesem Bereich vorgenommen. Aktivieren Sie die E-Mail-Benachrichtigung, indem Sie das Häkchen bei den jeweils meldbaren Ereignissen setzen. Über die **Begrenzung** kann ein übermäßiges Mailaufkommen im Fall eines massiven Virenbefalls verhindert werden.

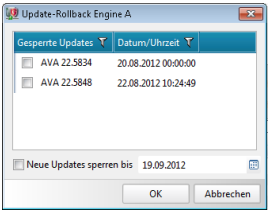


Um Änderungen an den **E-Mail-Einstellungen** vorzunehmen, klicken Sie bitte auf die Schaltfläche für erweiterte Einstellungen ( ).

Update-Rollback Engine A/B

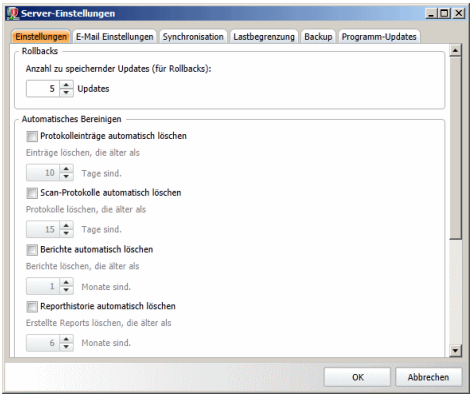
Es kann im seltenen Fall von Fehlalarmen oder ähnlichen Problemen sinnvoll sein, das aktuelle Update der Virensignaturen zu sperren und stattdessen eines der vorhergehenden Signaturupdates zu verwenden. Der G Data ManagementServer speichert von jeder AntiViren-Engine die letzten Updates. Sollte es also mit dem aktuellen Update der Engine A oder B Probleme geben, kann der Netzwerkadministrator das aktuelle Update für einen bestimmten Zeitraum sperren und stattdessen automatisch das zeitlich davorliegende Signaturupdate an die Clients und Subnet-Server verteilen. Die Anzahl der zu speichernden Rollbacks können Sie im Bereich **Server-Einstellungen** vornehmen. Standardmäßig werden die letzten fünf Signaturstände gespeichert.

> Auf Clients, die nicht mit dem G Data ManagementServer verbunden sind (z.B. Notebooks auf Dienstreisen) können keine Rollbacks durchgeführt werden. Eine vom Server an den Client übertragene Sperrung neuer Updates kann dort ohne Kontakt zum G Data ManagementSever nicht rückgängig gemacht werden.



Server-Einstellungen

Einstellungen



- **Rollbacks**: Geben Sie hier an, wie viele der aktualisierten Virensignaturupdates Sie für **Rollbacks** als Reserve vorhalten möchten. Als Standardwert gelten hier jeweils die letzten fünf Signatur-Updates der jeweiligen Engine.

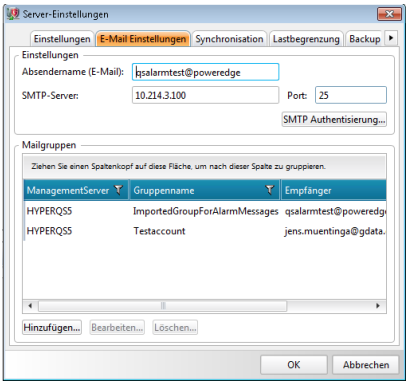
- **Automatisches Bereinigen**: Legen Sie hier fest, ob alte Updates automatisch nach einer gewissen Zeit gelöscht werden sollen.
  - **Protokolleinträge automatisch löschen**: Bestimmen Sie hier, dass Protokolleinträge nach einer gewissen Anzahl von Tagen gelöscht werden.
  - **Scan-Protokolle automatisch löschen**: Löschen Sie hier Scan-Protokolle, die älter als eine gewissen Anzahl von Tagen sind.
  - **Berichte automatisch löschen**: Legen Sie hier fest, dass Berichte nach einer gewissen Anzahl von Monaten gelöscht werden.
  - **Reporthistorie automatisch löschen**: Hier können Sie die Reporthistorie nach einer gewissen Anzahl von Monaten löschen.
  - **Clients nach Inaktivität automatisch löschen**: Löschen Sie hier Clients, wenn Sie eine gewisse Anzahl von Tagen nicht im Netzwerk eingeloggt waren.
  - **Patchdateien automatisch löschen**: Hier können Sie Patchdateien automatisch nach einer vorgebbaren Zeit löschen.

- **Authentifizierung für mobile Clients**: Definieren Sie hier das Passwort mit dem sich mobile Clients beim G Data ManagementServer authentifizieren.

E-Mail Einstellungen

Geben Sie hier den **SMTP-Server** und den **Port** (normalerweise 25) an, über den der G Data ManagementServer zum Versenden von Mails nutzen soll. Weiterhin wird eine (gültige) Absenderadresse benötigt, damit die Mails verschickt werden können. An diese E-Mail-Adresse werden auch die Antworten der Internet-Ambulanz geschickt.

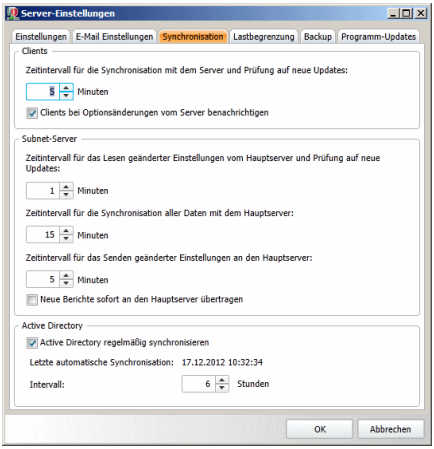
Unter **Mailgruppen** können Sie Listen verschiedener Empfänger verwalten, z.B. das Management-Team, Techniker usw.



Synchronisation

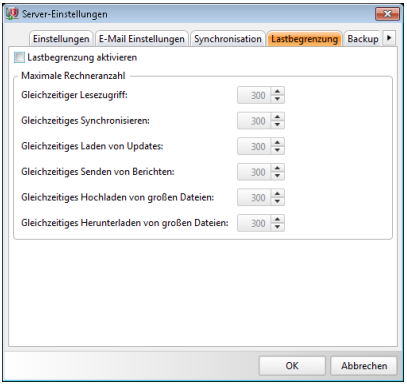
Im Synchronisation-Bereich können Sie das Synchronisationsintervall zwischen Clients, Subnet-Servern und Servern definieren:

- **Clients**: Geben Sie hier das Zeitintervall an, in dem die Clients mit dem Server synchronisiert werden. Als Standardwert sind fünf Minuten festgelegt. Wenn Sie das Häkchen bei **Clients bei Optionsänderungen vom Server benachrichtigen** setzen, werden die Client-Rechner direkt mit dem Server synchronisiert, unabhängig von vorgegebenen Synchronisationsintervallen.
- **Subnet-Server**: Über diesen Bereich können Sie die Intervalle für die Kommunikation zwischen Server und Subnet-Server definieren. Wenn Sie das Häkchen bei **Neue Berichte sofort an den Hauptserver übertragen** setzen, dann werden Berichte unabhängig von den hier vorgenommenen Einstellungen sofort an den Hauptserver übertragen.
- **Active Directory**: Legen Sie hier das Intervall fest, indem der G Data ManagementServer das Active Directory synchronisieren soll. Die Synchronisation des Active Directory erfolgt nur dann, wenn mindestens eine Gruppe einem Active Directory Eintrag **zugewiesen** wurde.



Lastbegrenzung

Wenn das Häkchen beim Eintrag **Lastbegrenzung aktivieren** gesetzt ist, lässt sich festlegen, wie viele Clients gleichzeitig die darunter aufgeführten Aktionen ausführen dürfen. So kann die Last verteilt werden, sodass es z.B. durch das gleichzeitige Laden von Updates zu keiner Latenzerhöhung im Netzwerk kommt.

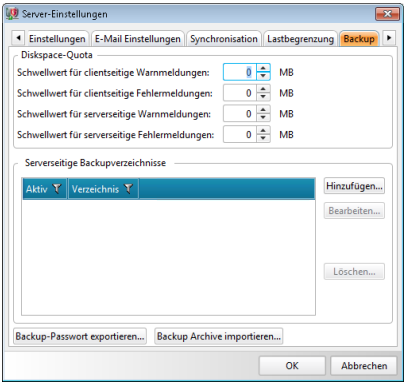


Backup

Im Bereich **Diskspace-Quota** werden Schwellenwerte für Warnungen eingestellt, die bei Erreichen der angegebenen Werte ausgegeben werden. Hier wird eingestellt, wie viel freier Speicherplatz auf dem Server frei sein muss, bevor eine Warnung oder eine Fehlermeldung ausgegeben wird. Dies ist sinnvoll, wenn beispielsweise für Anwendungen immer eine gewisse Menge Speicherplatz auf der Festplatte zur Verfügung stehen muss. Wird beispielsweise bei **Schwellwert für Clientseitige Warnmeldungen** der Wert 1500 angegeben, dann wird im G Data Administrator unter **Berichte** eine Warnung angezeigt, dass nur noch 1500 MB Speicherplatz verfügbar sind. Falls ein **Schwellwert für clientseitige Fehlermeldungen** angegeben wird, werden bei Erreichen des eingestellten Wertes ältere Backups gelöscht, um Speicherplatz für neue Backups zu schaffen. Dabei wird immer das älteste Backup zuerst gelöscht (FIFO-Prinzip).

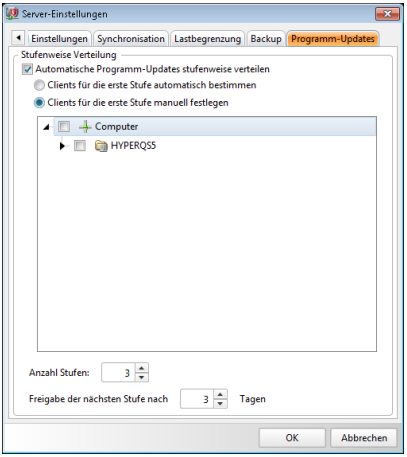
Darüber hinaus kann unter **Serverseitige Backupverzeichnisse** ein Pfad angegeben werden, auf dem alle auflaufenden Backups gespeichert werden sollen. Wird hier kein Verzeichnis angegeben, werden alle Backups unter **C:\ProgramData\G DATA \AntiVirus ManagementServer\Backup** bzw. **C:\Dokumente und Einstellungen \All Users\Anwendungsdaten\G DATA\AntiVirus ManagementServer\Backup** gespeichert.

Da sämtliche mit der G Data Software erstellten Backups verschlüsselt sind, besteht auch die Möglichkeit, die Passwörter für die Backups zu exportieren und für eine spätere Verwendung zu speichern. Über die Schaltfläche **Backup Archive importieren** ermöglicht den Zugriff auf Backups, die in anderen Ordnern gespeichert sind.



Programm-Updates

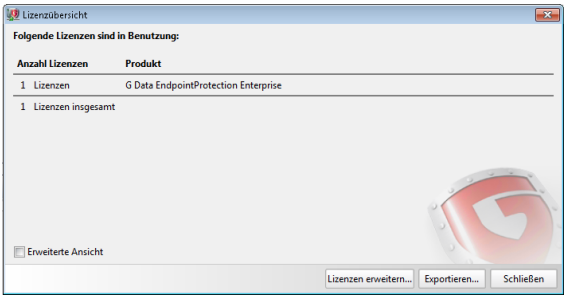
Im Bereich **Stufenweise Verteilung** können Sie festlegen, ob Sie Programmupdates zeitgleich auf allen Clients einspielen oder stufenweise. Eine stufenweise Verteilung verringert die Systemlast, die bei so einem Programmupdate unvermeidlich ist. Wenn Sie sich für eine stufenweise Verteilung entscheiden, können Sie festlegen, ob die Verteilung automatisch erfolgt oder selber festlegen, welche Clients zuerst mit Programm-Updates versehen werden sollen, welche Clients danach kommen und wie weit die Untergliederung in verschiedene Verteilungsstufen untergliedert ist.



Lizenzmanagement

Über das Lizenzmanagement haben Sie jederzeit Überblick darüber, wie viele Lizenzen Ihrer G Data Software in Ihrem Netzwerk installiert sind. Wenn Sie weitere Lizenzen benötigen, können Sie direkt über die Schaltfläche **Lizenzen erweitern** mit dem G Data Upgrade-Center Kontakt aufnehmen.

Über die Schaltfläche **Exportieren** haben Sie die Möglichkeit, sich eine Übersicht Ihrer verwendeten Lizenzen als Textdatei ausgeben zu lassen. Wenn Sie hier das Häkchen bei **Erweiterte Ansicht** setzen, erhalten Sie die Information darüber, auf welchem Server explizit welche Lizenzen eingesetzt werden.

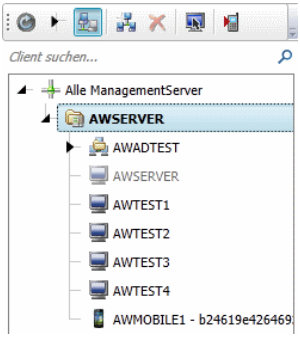


Hilfe

Hier erhalten Sie Informationen zum Programm und haben außerdem die Möglichkeit, auf die Online-Hilfe der G Data Software zurückzugreifen.

Clientauswahlbereich

Hier werden sämtliche Clients und Server sowie definierte Gruppen in Ihrem Netzwerk aufgelistet. Wie im Windows Explorer erscheinen Gruppen, in denen sich Untergliederungen befinden, mit einem kleinen Plus-Symbol. Wenn Sie dieses anklicken, öffnet sich die Verzeichnisstruktur an dieser Stelle und ermöglicht die Ansicht der darunter befindlichen Struktur. Ein Klick auf das Minus-Symbol schließt diese Untergliederung wieder. Zum Beispiel können Sie für PCs den Eintrag **Client-Einstellungen** aufrufen, um Ihre Optionen anzupassen. Bei mobilen Clients werden hingegen die **Mobile-Einstellungen** geöffnet.



Active Directory Integration

Über die Active Directory-Integration können alle Computerobjekte der Organisationseinheiten der Domäne importiert werden. Dazu muss eine eigene Gruppe im G Data Administrator angelegt werden. Nach einem Rechtsklick auf die neu erstellte Gruppe wird der Menüpunkt **Active Directory Eintrag der Gruppe zuordnen** sichtbar. Im Dialogfenster, das sich öffnet, wählen Sie den Punkt **Einer Gruppe im Active Directory zuweisen** aus und geben den LDAP-Server an. Die **Auswahl**-Schaltfläche stellt eine Auswahl verfügbarer Server zur Verfügung. Auch das Verbinden mit einer anderen Domäne ist möglich. Die Option **G Data Client automatisch auf neu hinzugefügten Rechnern installieren** bewirkt dass auf jedem Rechner, der zur Active Directory-Domäne zugefügt wird, sofort der Client installiert wird, sofern er die **Mindestvoraussetzungen** erfüllt. Der G Data ManagementServer gleicht seinen Datenstand regelmäßig mit dem Active Directory ab. Den Turnus, in dem der Datenstand abgefragt wird, kann individuell unter **Server-Einstellungen** > **Synchronisation** eingestellt werden.

Verzeichnisauswahl und Symbolleiste

Folgende Symbole sind in der Verzeichnisauswahl sichtbar:

Netzwerk

Gruppe

Server (aktiviert)

Server (deaktiviert)

Client (aktiviert)

Client (deaktiviert)

Linux-Client (aktiviert)

Linux-Client (deaktiviert)

Linux-Server (aktiviert)

Linux-Server (deaktiviert)

Laptop-Client (aktiviert)

Laptop-Client (deaktiviert)

Mobile-Client (aktiviert)

Mobile-Client (deaktiviert)

Nicht auswählbare Geräte: Hierunter fallen z.B. Netzwerkdrucker

In der Symbolleiste finden Sie die wichtigsten Befehle der **Organisation-Menüleiste** als anklickbare Symbole.

Ansicht aktualisieren: Über Aktualisieren oder die Taste **F5** können Sie die Ansicht der Administratoroberfläche jederzeit aktualisieren, um z.B. auch aktuelle Änderungen bei der Ansicht zu berücksichtigen.

Alles erweitern/reduzieren: Hiermit können Sie die Ansicht Ihres Netzwerksverzeichnisses beeinflussen.

Deaktivierte Clients anzeigen: Wählen Sie diese Schaltfläche, um auch die nicht aktivierten Computer anzuzeigen. Sie erkennen die deaktivierten Computer an den grau durchscheinenden Icons. Computer ohne Dateifreigabe bzw. Druckerfreigabe werden normalerweise nicht angezeigt.

Neue Gruppe: Die aktivierten Computer können zu **Gruppen** zusammengefasst werden. Damit lassen sich leicht unterschiedliche Sicherheitszonen definieren, da alle Einstellungen sowohl für einzelne Clients als auch für komplette Gruppen durchgeführt werden können. Zum Anlegen einer neuen Gruppe markieren Sie zunächst die übergeordnete Gruppe und klicken dann auf das abgebildete Symbol.

Löschen: Sie können einen Computer aus der Liste entfernen, indem Sie ihn markieren und dann die Schaltfläche Löschen anklicken. Beachten Sie, dass das Löschen eines Computers aus der Clientliste nicht dazu führt, dass die Client-Software deinstalliert wird.

Client aktivieren: Zum Aktivieren eines Computers, markieren Sie ihn in der Liste und wählen dann die abgebildete Schaltfläche.

Installationslink an mobile Clients senden: Um mobile Clients über den G Data Administrator zu verwalten, können Sie diesen einen Installationslink für die G Data MobileSecurity App per Mail schicken. Hierüber starten Sie dann die **Installation der G Data MobileSecurity**.

Organisation

Clients können über den **Clientauswahlbereich** auf der linken Seite der Programmoberfläche verwaltet werden. Erweiterte Optionen können Sie im Organisation-Menü durchführen.

Aktualisieren

Um Änderungen im Netzwerk zu verfolgen, die sich zu der Zeit ergeben, in der Sie den G Data Administrator nutzen, können Sie die **Aktualisieren**-Funktion verwenden.

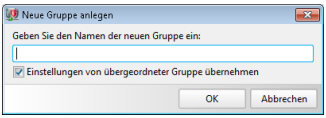
Deaktivierte Clients anzeigen

Clients, die nicht aktiviert sind, können über diese Funktion wieder sichtbar gemacht werden. Deaktivierte Clients werden dabei als durchscheinende Symbole dargestellt.

Im Gegensatz dazu sind aktivierte Clients durch vollfarbige Symbole gekennzeichnet.

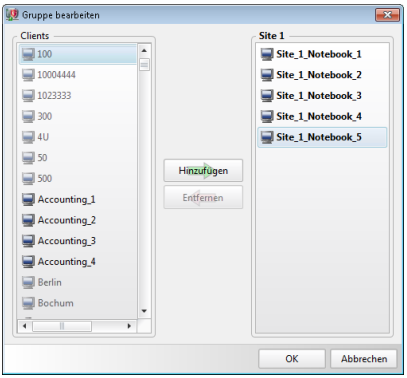
Neue Gruppe anlegen

Über diesen Befehl lässt sich eine Gruppe anlegen. Clients können in Gruppen zusammengefasst und ihre Einstellungen gruppenweise festgelegt werden. Nach dem Anwählen dieser Option und der Vergabe eines Gruppennamens können Clients der neuen Gruppe zugeordnet werden, indem man in der Clientliste den gewünschten Client mit der Maus, per Drag&Drop, auf die entsprechende Gruppe zieht.



Gruppe bearbeiten

Diese Option öffnet eine Dialogbox, in der sich über die Tasten **Hinzufügen** und **Entfernen** Clients zur Gruppe hinzufügen oder aus der Gruppe entfernen lassen. Nur verfügbar, wenn im Clientauswahlbereich eine Gruppe angewählt ist.



Löschen

Einzelne Clients lassen sich mit dem Befehl Löschen aus der Clientliste entfernen. Durch das Entfernen des Clients aus der Liste wird der G Data Client nicht deinstalliert.

> Um eine Gruppe zu löschen, müssen alle in ihr enthaltenen Clients nach Bedarf entweder deaktiviert oder in andere Gruppen verschoben werden. Nur leere Gruppen können gelöscht werden.

G Data Client Installationspaket erstellen

Über diese Funktion ist es möglich, ein Installationspaket für den G Data Security Client zu erstellen. Mit diesem Installationspaket können Sie den G Data Security Client lokal ohne Benutzerinteraktion einfach im Hintergrund installieren. Lesen Sie das Kapitel **Lokale Installation** für weitere Informationen.

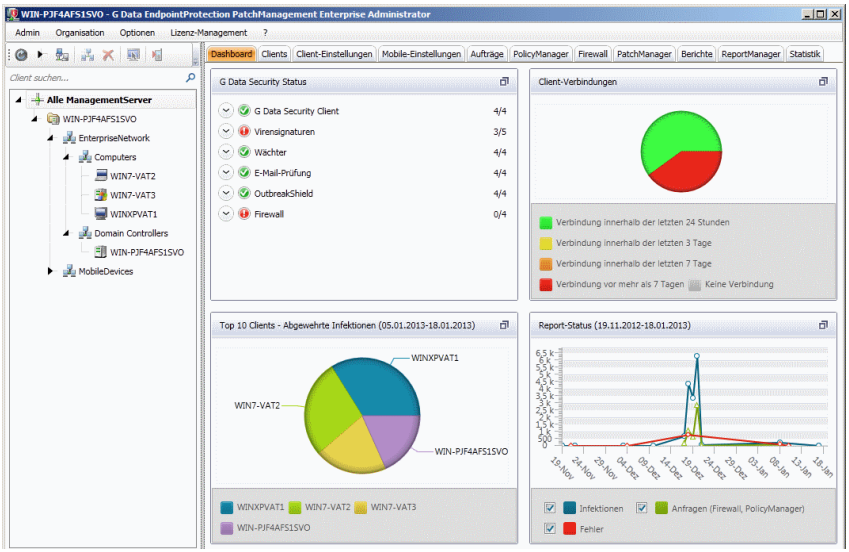
Aufgabenbereiche

In den verschiedenen Aufgabenbereichen, die über die jeweiligen Karteireiter anwählbar sind, besteht die Möglichkeit, die Absicherung des gesamten Unternehmensnetzwerks und seiner Clients zu administrieren. Die Einstellungen, die dabei vorgenommen werden, beziehen sich immer auf die Clients oder Gruppen, die im **Clientauswahlbereich** markiert wurden. Die einzelnen Themenfelder werden in den folgenden Abschnitten eingehend erläutert.

Für die meisten Module gibt es allgemeine Optionen, um das Layout und den Inhalt der Listen im Infobereich zu editieren. Zum Beispiel kann die Anzahl der Einträge pro Seite reduziert werden. Wählen Sie hierzu die maximale **Anzahl pro Seite** am unteren rechten Rand der Programmoberfläche aus. Für die Eingabe von Freitext-Filtern klicken Sie auf eine der Filter-Schaltflächen in den Spaltenüberschriften und geben Sie dort Ihre Filterkriterien ein. Neben dem Filter können Sie Listenelemente auch durch die Verwendung von Gruppen sortieren. Ziehen Sie dazu eine oder mehrere Spaltenüberschriften auf die Leiste oberhalb der Spaltenüberschriften, um eine Gruppe aus dieser Spalte zu erstellen. Gruppen können in unterschiedlicher Weise und in unterschiedlichen Ansichten erzeugt und verschachtelt werden.

Dashboard

Im Dashboard-Bereich der G Data Software erhalten Sie Informationen zum aktuellen Zustand der Clients im Netzwerk. Diese finden sich rechts vom jeweiligen Eintrag als Text-, Zahl- oder Datumsangabe.



G Data Security Status

Hier können Sie alle grundlegenden Sicherheitseinstellungen für die Clients oder Gruppen einstellen, die Sie im Clientauswahlbereich markiert haben.

Solange das Netzwerk optimal für den Schutz vor Computerviren konfiguriert ist, finden Sie links vor den hier aufgeführten Einträgen ein grünes Symbol.

Sollte mindestens eine Komponente nicht optimal eingestellt sein (z.B. abgeschalteter Wächter oder veraltete Virensignaturen), weist ein Achtung-Symbol darauf hin.

Wenn sich die G Data-Programmoberfläche öffnet, sind in einigen Fällen für kurze Zeit die meisten Symbole im Info-Modus. Das heißt nicht, dass das Netzwerk in diesem Moment ungeschützt ist. Hier handelt es sich um eine interne Überprüfung des Virenschutz-Status. In diesem Moment wird die Datenbank des G Data ManagementServers vom G Data Administrator abgefragt.

Durch Anklicken des jeweiligen Eintrags können Sie hier direkt Aktionen vornehmen oder in den jeweiligen Aufgabenbereich wechseln. Sobald Sie die Einstellungen einer Komponente mit Achtung-Symbol optimiert haben, wechselt das Symbol im Status-Bereich wieder auf das grüne Symbol.

Client-Verbindungen

Hier erhalten Sie eine zeitliche Übersicht über die Verbindungen, die die jeweiligen Clients oder Gruppen mit dem G Data ManagementServer hatten. Es sollte darauf geachtet werden, dass sich alle Clients regelmäßig mit dem G Data ManagementServer verbinden.

Top 10 Clients - Abgewehrte Infektionen

Die Clients die z.B. aufgrund des Nutzerverhaltens oder technischer Umstände in dieser Liste erscheinen, sollten besonders beobachtet werden. Ein Auftauchen eines oder mehrerer Clients in diesem Bereich ist unter Umständen eine Indikation dafür, dass der Client-Anwender auf eventuelle Probleme aufmerksam gemacht werden oder technische Maßnahmen ergriffen werden sollten. Wenn die Infektionen auf Grund des Nutzerverhaltens stattfinden, wäre z.B. eine Nutzung des **PolicyManagers** (verfügbar in der Programmversion **G Data EndpointProtection**) ratsam.

Report-Status

Hier erhalten Sie eine übersichtliche Darstellung über die Menge der Infektionen, Anfragen und Fehler in Ihrem Netzwerk innerhalb der letzten 30 Tage.

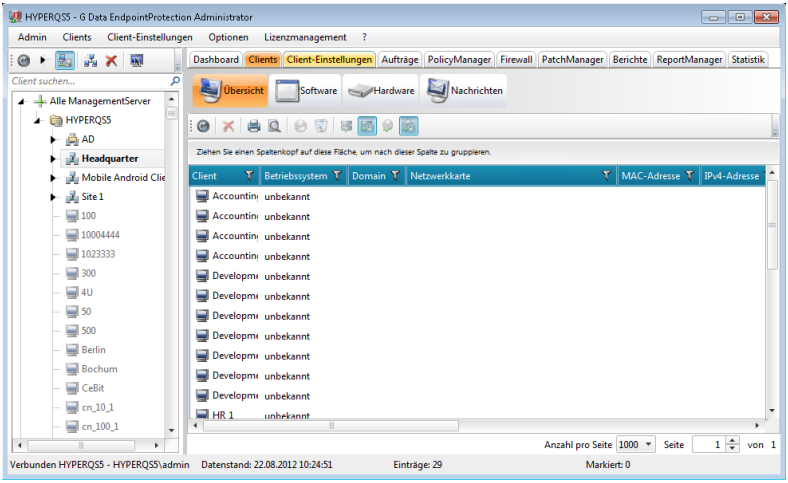
Clients

Wählen Sie im **Clientauswahlbereich** eine Gruppe, um eine Übersicht über alle Clients der Gruppe zu erhalten. Für jeden Client wird angezeigt, welche Version der installierte Client hat, welche Version die Virensignaturen haben und wann der Client sich zum letzten Mal beim G Data ManagementServer gemeldet hat. Hier lässt sich überprüfen, ob die Clients ordnungsgemäß laufen und ob die Virensignaturen auf dem neuesten Stand sind.

Über die oben befindlichen Schaltflächen können Sie entscheiden, ob Sie eine allgemeine **Übersicht** über die Clients bearbeiten möchten oder ob Sie den einzelnen Clients **Nachrichten** senden möchten. Mit dem Versand dieser Nachrichten können Sie Anwender schnell und unkompliziert über Änderungen am Status des Clients informieren. Über das Client-Modul erhalten Sie außerdem eine grundlegenden Übersicht über die auf dem Client installierte **Hardware** und **Software**.

Übersicht

Hier erhalten Sie eine Übersicht über alle verwalteten Clients und können diese gleichzeitig auch administrieren.



Mit einem rechten Mausklicke auf die Spaltenüberschriften können Sie weitergehende Informationsspalten zum Client zu- oder abwählen:

- Server
- Alias (server)
- Client
- Engine A
- Engine B
- Datenstand
- Version G Data Security Client
- Sprache
- UPMS-Client
- Letzter Zugriff
- Update Virendatenbank / Zeitpunkt

- Update Programmdateien / Zeitpunkt
- Betriebssystem
- Subnet-Server
- Domain
- Netzwerkkarte
- MAC-Adresse
- IPv4-Adresse
- IPv6-Adresse
- Subnetz-Maske
- Standardgateway
- DNS-Server
- DHCP-Server
- PrimaryWINS
- SecondaryWINS

Zur Administration der Clients und Gruppen stehen Ihnen folgende Schaltflächen zur Verfügung.

Aktualisieren: Diese Funktion aktualisiert die Ansicht und lädt die aktuellen Client-Liste vom G Data ManagementServer.

Löschen: Hiermit entfernen Sie einen Client aus der Clientübersicht.

Drucken: Hiermit starten Sie den Druckvorgang für die Client-Übersicht. Sie können in dem erscheinenden Auswahlfenster bestimmen, welche Details und Bereiche der Clients Sie ausdrucken möchten.

Seitenansicht: Hier können Sie vor dem eigentlichen Ausdruck eine Vorschau der zu druckenden Seiten am Monitor ausgeben.

G Data Client installieren

G Data Client deinstallieren

Virendatenbank aktualisieren: Aktualisiert die Virendatenbank auf dem Client mit den Dateien vom G Data ManagementServer.

Virendatenbank automatisch aktualisieren: Aktiviert die automatische Aktualisierung der Virendatenbank. Die Clients prüfen periodisch, ob aktualisierte Virensignaturen auf dem G Data ManagementServer vorhanden sind und führen die Aktualisierung automatisch durch.

Programmdateien aktualisieren: Aktualisiert die Programmdateien auf dem Client. Es werden die Client-Programmdateien verwendet, die der G Data ManagementServer bereit hält. Nach der Aktualisierung der Programmdateien kann es sein, dass der Client neu gestartet werden muss.

Programmdateien automatisch aktualisieren: Aktiviert die automatische Aktualisierung der Programmdateien. Die Clients prüfen periodisch, ob eine neue Version auf dem G Data ManagementServer existiert und führen die Aktualisierung automatisch durch.

Menüleiste

Wenn Sie die Option **Übersicht** ausgewählt haben, erscheint hier ein zusätzlicher Menü-Eintrag namens **Clients**. Hier finden Sie die Funktionen wieder, die Sie auch durch Anklicken eines oder mehrerer Clients mit der rechten Maustaste im Kontextmenü erhalten würden. Folgende Optionen stehen hier zur Verfügung:

- **G Data Security Client installieren**
- **G Data Security Client für Linux installieren**
- **G Data Security Client deinstallieren**
- **Auf Gruppeneinstellungen zurücksetzen**: Hiermit führen Sie ein Reset der Sicherheitseinstellungen für einen modifizierten Client auf die vorgegebenen Gruppeneinstellungen durch.
- **G Data Security Client in Gruppe verschieben**: Diese Funktion ermöglicht es Ihnen, ausgewählte Clients in eine existierende Gruppe zu verschieben. Wenn Sie diese Option auswählen, werden alle existierenden Gruppen in einem neuen Fenster angezeigt. Um nun den Client in eine Gruppe zu verschieben, wählen Sie die in Frage kommende Gruppe aus und klicken Sie auf OK.
- **G Data Subnet-Server zuordnen**: Wenn Sie die Möglichkeit haben, Clients speziellen Subnet-Servern über die Funktion Server verwalten zuzuweisen, haben Sie auch die Option diesen Vorgang über das Kontextmenü durchzuführen.
- **Virendatenbank jetzt aktualisieren**
- **Virendatenbank automatisch aktualisieren**
- **Programmdateien jetzt aktualisieren**
- **Programmdateien automatisch aktualisieren**

- **Neustart nach Aktualisierung der Programmdateien**: Legen Sie hier fest, wie der Client reagieren soll, nachdem die Programmdateien aktualisiert wurden. Wählen Sie die Option **Hinweisfenster auf dem Client anzeigen**, um den Anwender darüber zu informieren, dass er in nächster Gelegenheit seinen Rechner neu starten sollte, damit das Programm-Update durchgeführt werden kann. Über **Bericht** erzeugen erhalten Sie im Berichte-Bereich Infos darüber, welche Clients aktualisiert wurden. Mit der Option **Neustart ohne Abfrage durchführen** können Sie das Update automatisch auf den Clients einspielen und diese zu einem Neustart zwingen.

G Data Security Client installieren

Wählen Sie die Option **G Data Security Client installieren**, um die **Remote-Installation** des G Data Security Clients auf allen ausgewählten Rechnern durchzuführen.

> Um auf deaktivierte Clients zugreifen zu können, müssen diese in der Clientübersicht als aktiv angezeigt werden. Bei Verwendung der Funktion G Data Security Client installieren weist Sie das Programm gegebenenfalls darauf hin und ermöglicht eine Darstellung der deaktivierten Clients.

Sollte die Software nicht über die Remote-Installation auf den Clients aufgespielt werden können, haben Sie die Möglichkeit direkt am Clientrechner eine **lokale Installation** mit der G Data Software DVD oder einem Client-Installationspaket durchzuführen.

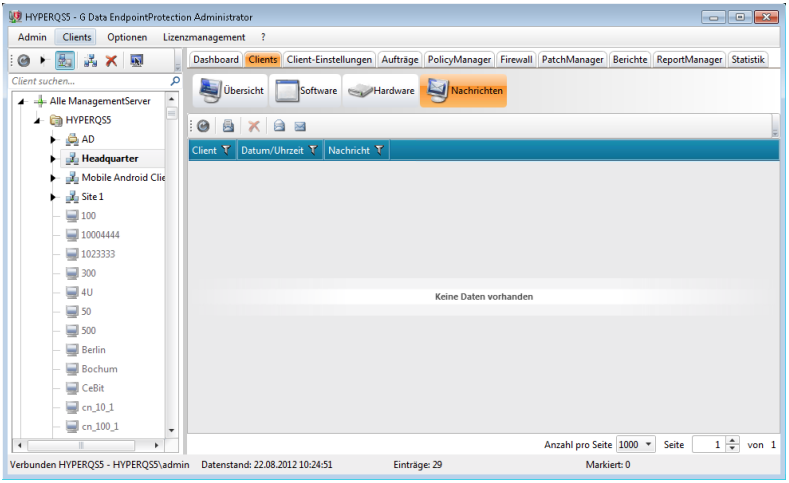
G Data Security Client deinstallieren

Diese Funktion erteilt dem G Data Security Client den Auftrag, sich selbst zu deinstallieren. Zum vollständigen Entfernen muss der Client neu gestartet werden. Der Anwender wird durch eine Meldung dazu aufgefordert.

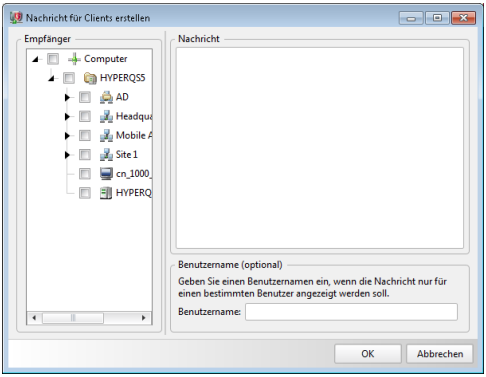
Alternativ ist es auch möglich, den Client lokal per Kommandozeilenbefehl zu deinstallieren. Hierzu ist eine Eingabeaufforderung mit Administratorberechtigungen erforderlich. Wird im Verzeichnis **C:\Programme (x86)\G DATA\AVKClient** der Befehl **UnClient /AVKUninst** abgesetzt, startet die Deinstallation. Gegebenenfalls wird ein Neustart verlangt. Sollte eine solche Anfrage nicht erscheinen, muss der Rechner nach max. 10 Minuten neu gestartet werden.

Nachrichten

Sie als Netzwerkadministrator können an einzelne Clients oder Client-Gruppen Nachrichten versenden. Mit dem Versand dieser Nachrichten können Sie Anwender schnell und unkompliziert über Änderungen am Status des Clients informieren. Die Nachrichten werden dabei als Info unten rechts auf dem Desktop des Client-Rechners angezeigt.



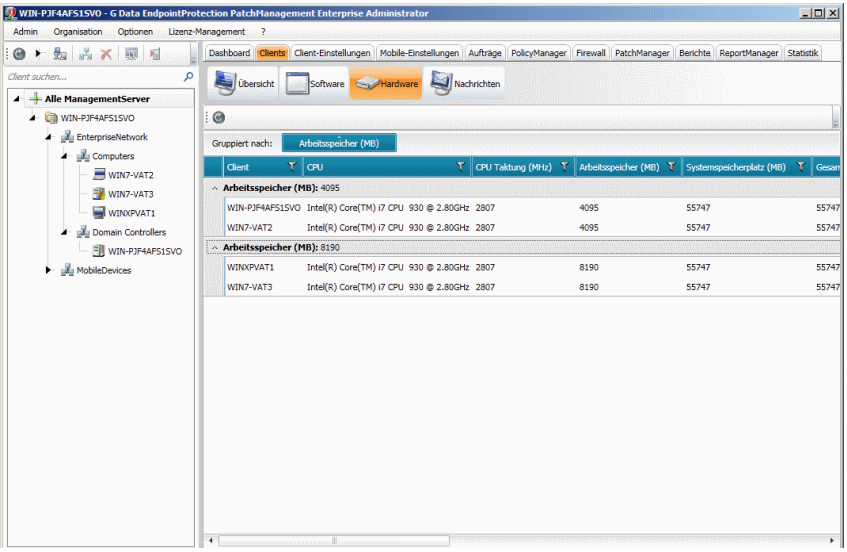
Um eine neue Nachricht zu erzeugen, klicken Sie einfach mit der rechten Maustaste in die Spaltenansicht und wählen **Neue Nachricht**. In dem nun erscheinenden Kontext-Dialog können Sie die Clients, denen Sie die Nachricht senden möchten, per Häkchen zu- oder abwählen.



Wenn Sie eine Nachricht nur bestimmten Benutzern eines Client-Rechners oder Netzwerks zugängig machen möchten, geben Sie dessen Anmeldenamen unter **Benutzername** ein. Tippen Sie nun in dem Feld **Nachricht** Ihre Hinweise für die Clients ein und drücken Sie dann auf die Schaltfläche **Senden**.

Hardware Inventar

Über diese Ansicht erhalten Sie Informationen zu der von den Clients verwendeten Hardware.



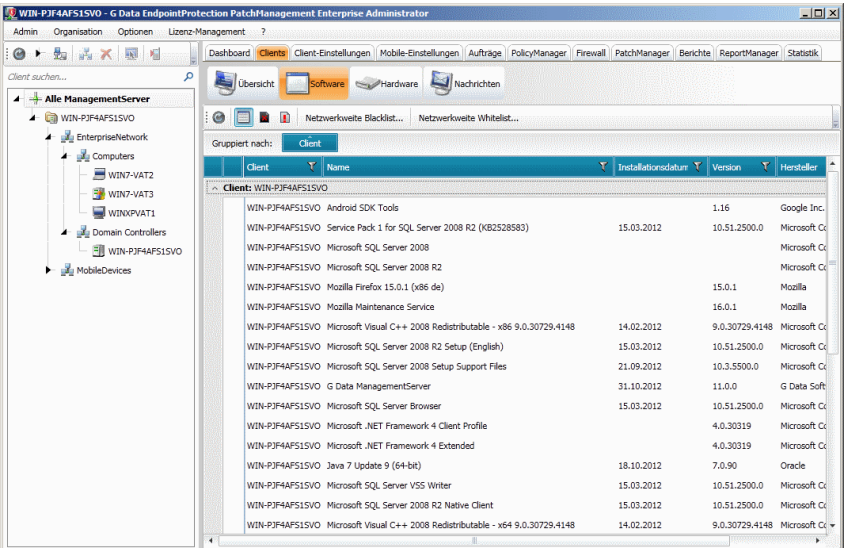
Mit einem rechten Mausklicke auf die Spaltenüberschriften können Sie weitergehende Informationsspalten zur Software zu- oder abwählen:

- Client
- CPU
- CPU Taktung (MHz)
- Arbeitsspeicher (MB)
- Systemspeicherplatz (MB)
- Systemspeicherplatz (Statistik)
- Gesamtspeicherplatz (MB)
- Gesamtspeicherplatz (Statistik)
- Systemhersteller
- Systemname

- Systemversion
- Systemfamilie
- CPU-ID
- Mainboardhersteller
- Mainboard
- Mainboardversion
- Bios Hersteller
- Bios Veröffentlichungsdatum
- Bios Version

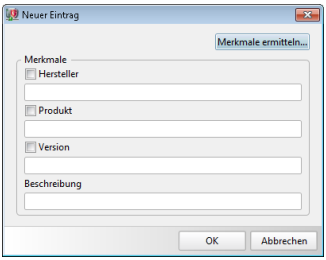
Software Inventar

Das Software Inventar erlaubt Ihnen, die Software-Nutzung im gesamten Netzwerk zu überwachen. Software kann dabei auf Blacklists oder Whitelists hinzugefügt werden, um Software-Management im Netzwerk zu unterstützen.



In der Listenansicht wird installierte Software für alle Clients im **Clientauswahlbereich** aufgelistet. Um die Whitelist bzw. Blacklist zu füllen, klicken Sie bitte auf die Schaltfläche **Netzwerkweite Blacklist** bzw. **Netzwerkweite Whitelist** und in dem nun erscheinenden Fenster auf die Schaltfläche **Hinzufügen**. Die Option **Merkmale ermitteln** können Sie Programme auswählen, die Sie auf eine Blacklist oder Whitelist setzen möchten und die zugehörigen Attribute eingeben, mit denen das jeweilige Programm ermittelt werden kann. Um ein Attribut als Regel zu nutzen, setzen Sie einfach das Häkchen an das entsprechende Kästchen. Auf diese

Weise können Sie z.B. Software bestimmter Hersteller oder auch nur spezielle Programmversionen black- oder whitelisten. Wenn Ihnen die erforderlichen Daten zur Verfügung stehen, können Sie Software auch durch Direkteingabe der Merkmale (ohne Umweg über **Merkmale ermitteln**) auf die Black- oder Whitelist setzen.



Die Übersicht über die Elemente auf Ihrer Black-/Whitelist können Sie mit folgenden Schaltflächen beeinflussen.

Aktualisieren: Diese Funktion aktualisiert die Ansicht und lädt die aktuellen Clienteinstellungen vom G Data ManagementServer.

Alle anzeigen: Hiermit wird Ihnen sämtliche im Netzwerk auf den Clients installierte Software angezeigt.

Nur Software auf der Blacklist anzeigen: Über diese Einstellung können Sie sich die Software anzeigen, die durch Ihren Eintrag auf der Blacklist auf den Clients nicht ausgeführt werden kann.

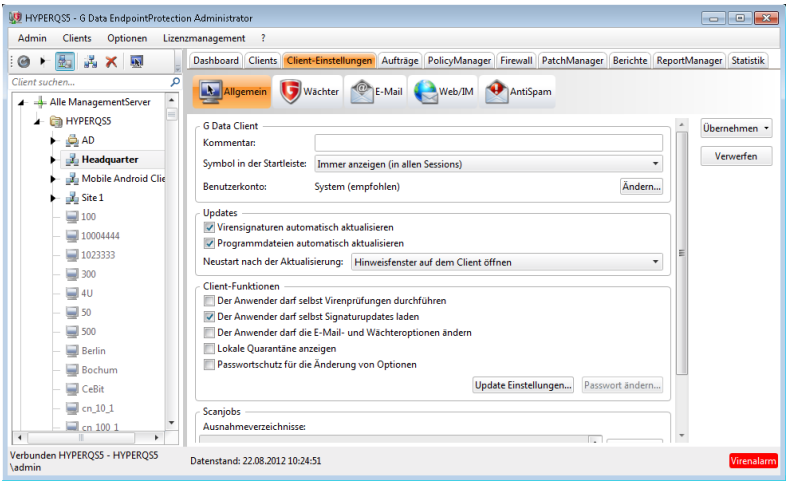
Nur Software anzeigen, die nicht auf der Whitelist ist: Hiermit erhalten Sie einen Überblick über installierte Software auf den Netzwerk-Clients, die vom Netzwerkadministrator noch nicht überprüft und kategorisiert wurde. Mit Hilfe dieser Ansicht können Sie gefundene Software mit einem Rechtsklick auf die Whitelist oder Blacklist setzen.

Client-Einstellungen

In diesem Modul können Sie die Parameter für jeden einzelnen Client bzw. jede Gruppe von Clients managen. In dem Sie die Karteireiter Allgemein, Wächter, E-Mail, Web/IM und AntiSpam nutzen, können Sie Ihre Clients ganz individuell auf die Bedürfnisse Ihres Netzwerks und dessen Benutzer optimieren.

Allgemein

In diesem Bereich können Sie die grundlegenden Einstellungen der ausgewählten Clients bearbeiten.



G Data Security Client

- **Kommentar**: Geben Sie hier ggf. ergänzende Informationen zum Client ein.
- **Symbol in der Startleiste**: Für Terminal-Server und Windows mit schneller Benutzerumschaltung kann gewählt werden, in welchen Sessions ein Client-Symbol in der Taskleiste angezeigt werden soll: **nie**, **nur in der ersten Session** (für Terminalserver) oder **immer**. Bei normalen Clients kann mit der Option das Anzeigen des Client-Symbols wahlweise unterbunden werden. Damit der Anwender Zugriff auf erweiterte Client-Optionen, wie z.B. den Leerlauf-Scan hat, muss das Symbol angezeigt werden.
- **Benutzerkonto**: Die Client-Software läuft normalerweise im Systemkontext. Sie können hier ein anderes Konto angeben, um die Prüfung von Netzwerkverzeichnissen zu ermöglichen. Das Konto muss dazu Administratorrechte auf dem Client haben.

Updates

- **Virensignaturen automatisch aktualisieren**: Aktiviert die automatische Aktualisierung der Virendatenbank. Die Clients prüfen periodisch, ob aktualisierte Virensignaturen auf dem ManagementServer vorhanden sind. Liegen aktualisierte Virensignaturen vor, werden diese auf dem Client automatisch installiert.
- **Programmdateien automatisch aktualisieren**: Aktiviert die automatische Aktualisierung der Client-Programmdateien. Die Clients prüfen periodisch, ob aktualisierte Programmdateien auf dem ManagementServer vorhanden sind. Liegen aktualisierte Programmdateien vor, werden diese auf dem Client automatisch installiert. Nach der Aktualisierung der Programmdateien kann es sein, dass der Client neu gestartet werden muss. Je nach Einstellung unter **Neustart nach der Aktualisierung** hat der Anwender auf dem Client die Möglichkeit, den Abschluss der Aktualisierung auf einen späteren Zeitpunkt zu verschieben.
- **Neustart nach der Aktualisierung**: Wählen Sie **Hinweisfenster auf dem Client anzeigen** um den Anwender darüber zu unterrichten, dass er seinen Client-Rechner in nächster Zeit neu starten sollte, damit das Update eingespielt werden kann. **Bericht erzeugen** erzeugt einen Bericht im Bereich **Berichte**. Über die Funktion **Neustart ohne Abfrage durchführen** wird auf dem Client-Rechner ungefragt automatisch ein Neustart durchgeführt.
- **Update-Einstellungen**: Hier wird festgelegt, woher die Clients ihre Virensignaturupdates beziehen. Es besteht die Möglichkeit, Clients unterschiedslos vom ManagementServer die Virensignaturen laden zu lassen; alternativ kann das Recht eingeräumt werden, selbst die Aktualisierungen durchzuführen. Für mobile Arbeitsplätze empfiehlt sich ein Mischbetrieb, d.h. solange der Client eine Verbindung zum ManagementServer hat, bezieht er die Aktualisierungen von dort. Besteht keine Verbindung zum ManagementServer mehr, werden die Virensignaturen automatisch aus dem Internet geladen. Über die Schaltfläche **Einstellungen und Zeitplanung** können des Weiteren für den jeweiligen Client Einstellungen vorgenommen werden, je nach Einsatzumgebung erforderlich sind, um den Download der Virensignaturen zu ermöglichen. Auch die Intervalle, in denen Aktualisierungen vorgenommen werden, können hier definiert werden.

Client-Funktionen

Im Folgenden werden die Berechtigungen vergeben, die der Benutzer lokal für einzelne Clientfunktionen hat. So können dem Anwender umfangreiche oder auch nur stark eingeschränkte Rechte zur Änderung von Einstellungen eingeräumt werden

- **Der Anwender darf selbst Virenprüfungen durchführen**: Im akuten Verdachtsfall kann der Anwender wie bei einer lokal installierten Antivirenlösung auf seinem Rechner unabhängig vom ManagementServer eine **Virenprüfung** durchführen. Ergebnisse dieser Virenprüfung werden beim nächsten Kontakt mit dem ManagementServer an diesen übermittelt.

- **Der Anwender darf selbst Signaturupdates laden**: Wenn Sie diese Funktion aktivieren, darf der Nutzer des Clientrechners aus dem Kontextmenü heraus Virensignaturen auch ohne Verbindung zum ManagementServer direkt aus dem Internet laden.
- **Der Anwender darf die E-Mail- und Wächteroptionen ändern**: Wenn diese Funktion aktiviert ist, hat der Benutzer des Client-Rechners die Möglichkeit, Einstellungen in folgenden Bereichen für seinen Client zu ändern: **Wächter**, **Email**, **Web/IM** und **AntiSpam**.
- **Lokale Quarantäne anzeigen**: Wenn das Anzeigen der lokalen **Quarantäne** erlaubt wird, kann der Anwender Daten, die vom Wächter wegen Virenbefall oder -verdacht in Quarantäne geschoben wurden ggf. desinfizieren, löschen oder zurückbewegen. Beachten Sie dabei, dass bei einem Zurückbewegen einer Datei aus der Quarantäne ein Virus nicht entfernt wird. Diese Option sollte deshalb nur versierten Anwendern auf den Clients zugänglich gemacht werden.
- **Passwortschutz für die Änderung von Optionen**: Um einer missbräuchlichen Manipulation von lokalen Einstellungen vorzubeugen, gibt es die Möglichkeit, die Änderung von Optionen nur dann zuzulassen, wenn ein Passwort eingegeben wird. So lässt sich beispielsweise verhindern, dass ein User, der normalerweise nicht am betroffenen Client arbeitet, die Einstellungen ändert. Das Passwort kann individuell für den jeweiligen Client oder die jeweilige Gruppe vergeben werden; darauf muss nur den autorisierten Nutzern dieses Passwort mitgeteilt werden.

Scanjobs

Sie können hier Ausnahmen definieren, die nicht während der Ausführung der Scan-Aufträge überprüft werden. Zum Beispiel können Archiv- und Backup-Bereiche einer Festplatte oder Partition als Ausnahmen definiert werden, auch bestimmte Ordner oder sogar Dateierweiterungen können von den Scanjobs ausgeschlossen werden. Diese Ausnahmen können auch für komplette Gruppen definiert werden. Falls die Clients in einer Gruppe unterschiedliche Ausnahmeverzeichnisse definiert haben, können neue Verzeichnisse hinzugefügt oder vorhandene gelöscht werden. Die speziell für einzelne Clients definierten Verzeichnisse bleiben dabei erhalten. Das gleiche Verfahren wird auch bei den Wächterausnahmen angewendet.

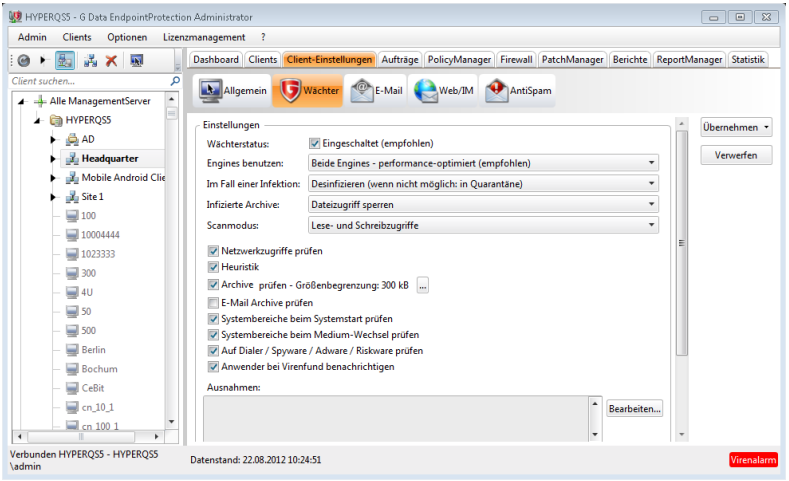
Durch Anklicken der **Analyse-Umfang**-Schaltfläche können Sie den Scan-Bereich festlegen. Standardmäßig sind hier alle lokalen Festplattenlaufwerke eingestellt. Wenn Sie möchten, dass der Client einen Virenscan durchführen soll, wenn sich der Computer im Leerlauf befindet, wählen Sie die Option **Leerlauf-Scan**.

> Besonderheit auf einem Linux-Fileserver: Bei der Auswahl von Ausnahmeverzeichnissen werden das Root-Laufwerk (/) und alle Freigaben zurück geliefert. Dabei können Laufwerks-, Verzeichnis- und Dateiausnahmen angelegt werden.

Wächter

Hier können die Wächtereinstellungen für den im **Clientauswahlbereich** gewählten Client bzw. die ausgewählte Gruppe vorgenommen werden. Die geänderten Einstellungen werden erst nach Betätigung der **Übernehmen**-Schaltfläche gespeichert. Drücken Sie die **Verwerfen**-Schaltfläche, um die aktuellen Einstellungen vom ManagementServer zu laden, ohne die Änderungen zu übernehmen. Sollten Client innerhalb einer Gruppe unterschiedliche Einstellungen haben, wird bei Parametern, die unterschiedlich eingestellt sind einzelne Parameter einen undefinierten Status einnehmen. Die Clients der Gruppe haben in diesem Fall unterschiedliche Einstellungen für die Parameter. Undefinierte Parameter werden beim Übernehmen nicht gespeichert.

Der Wächter sollte grundsätzlich nicht deaktiviert werden, da dieser für den Echtzeitschutz vor Schädlingen sorgt. Wird der Wächter deaktiviert, besteht dieser Schutz nicht mehr. Es wird daher empfohlen, den Wächter nur dann auszuschalten, wenn ein berechtigtes Interesse daran besteht, zum Beispiel Fehlersuche oder Diagnose. Die Definition von Ausnahmen für den Wächter ist möglich. Sollte eine Anwendung durch den Einsatz des Wächters mit Performanceeinbußen zu kämpfen haben, können für die entsprechenden Programmdateien, Prozesse oder Dateien Ausnahmen hinzugefügt werden; ausgenommene Dateien werden dann nicht mehr vom Wächter geprüft. Beachten Sie, dass das Hinzufügen von Wächterausnahmen unter Umständen ein Sicherheitsrisiko darstellen kann.



Einstellungen

- **Wächterstatus**: Hier können Sie den Wächter anschalten bzw. ausschalten. Generell sollten Sie den Wächter eingeschaltet lassen. Er ist die Grundlage für einen permanenten und lückenlosen Virenschutz.
- **Engines benutzen**: Die G Data Software arbeitet mit zwei unabhängig voneinander operierenden Virenanalyseeinheiten. Prinzipiell ist die Verwendung beider Engines der Garant für optimale Virenprophylaxe. Die Verwendung einer einzigen Engine bringt dagegen Performance-Vorteile mit sich.
- **Im Fall einer Infektion**: Hier können Sie festlegen, was bei Entdeckung einer infizierten Datei geschehen soll. Je nachdem, für welche Zwecke der jeweilige Client verwendet wird, sind hier unterschiedliche Einstellungen sinnvoll.
  - **Dateizugriff sperren**: Auf eine infizierte Datei können weder Schreib- noch Lesezugriffe ausgeführt werden.
  - **Desinfizieren (wenn nicht möglich: Zugriff sperren)**: Hier wird versucht, den Virus zu entfernen, falls das nicht möglich ist, dann wird der Dateizugriff gesperrt.
  - **Desinfizieren (wenn nicht möglich: in Quarantäne)**: Hier wird versucht, den Virus zu entfernen. Falls dies nicht möglich ist, wird die Datei in die Quarantäne verschoben.
  - **Desinfizieren (wenn nicht möglich: Datei löschen)**: Hier wird versucht, den Virus zu entfernen. Falls dies nicht möglich ist, wird die Datei gelöscht. Allerdings kann es dabei im seltenen Fall einer falsch-positiven Virenmeldung zu Datenverlust kommen.
  - **Datei in Quarantäne verschieben**: Hier wird die infizierte Datei in die Quarantäne verschoben. Eine mögliche Desinfektion der Datei kann dann manuell durch den Systemadministrator durchgeführt werden.
  - **Infizierte Datei löschen**: Als rigorose Maßnahme hilft diese Funktion dabei, den Virus wirkungsvoll einzudämmen. Allerdings kann es dabei im seltenen Fall einer falsch-positiven Virenmeldung zu Datenverlust kommen.
- **Infizierte Archive**: Legen Sie hier fest, wie infizierte Archive behandelt werden sollen. Beachten Sie beim Festlegen dieser Einstellungen, dass ein Virus innerhalb eines Archives erst dann Schaden anrichtet, wenn das Archiv entpackt wird.
- **Scanmodus**: Legen Sie hier fest, wie Dateien gescannt werden sollen. **Lesezugriffe** scannt jede Datei sofort, wenn Sie gelesen wird. **Lese- und Schreibzugriffe** überprüft Dateien nicht nur bei Lese- sondern auch bei Schreibzugriffen. Dies dient als Schutz vor Viren, die möglicherweise von einem anderen ungeschützten Client oder aus dem Internet kopiert werden. **Bei Ausführung** führt einen Scan durch, sobald eine Datei ausgeführt wird.

- **Netzwerkzugriffe prüfen**: Hier können Sie die Vorgehensweise des Wächters im Zusammenhang mit Netzwerkzugriffen festlegen. Wenn Sie ihr gesamtes Netzwerk generell mit der G Data Software überwachen, kann eine Überprüfung der Netzwerkzugriffe entfallen.
- **Heuristik**: In der heuristischen Analyse werden Viren nicht nur anhand der ständig aktualisierten Virendatenbanken ermittelt, sondern auch anhand bestimmter virentypischer Merkmale erkannt. Diese Methode ist einerseits ein weiteres Sicherheitsplus, andererseits kann in seltenen Fällen auch ein **Fehlalarm** erzeugt werden.
- **Archive prüfen**: Das Überprüfen gepackter Daten in Archiven ist sehr zeitintensiv und kann in der Regel dann unterbleiben, wenn der G Data Virenwächter auf dem System aktiv ist. Dieser erkennt dann beim Entpacken des Archives einen bis dahin verborgenen Virus und unterbindet automatisch dessen Verbreitung. Um die Performance durch das unnötige Überprüfung großer Archiv-Dateien, die selten verwendet werden, nicht zu belasten, können Sie die Größe der Archivdateien, die durchsucht werden, auf einen bestimmten Wert in Kilobyte begrenzen.
- **E-Mail Archive prüfen**: Diese Option sollte in der Regel ausgeschaltet werden, da die Prüfung von E-Mail-Archiven in der Regel sehr lange dauert und im Falle einer infizierten Mail eine Mailbox - abhängig von den Einstellungen des Virenscans - in die Quarantäne verschoben oder gelöscht wird. Mall Mails innerhalb des Mailarchivs sären in einem solchen Fall nicht mehr verfügbar. Da der Wächter die Ausführung von infizierten E-Mail-Anhängen blockiert, wird durch das Ausschalten dieser Option kein Sicherheitsloch geschaffen. Bei der Verwendung von Outlook werden die ein- und ausgehenden Mails zusätzlich durch ein integriertes Plugln geprüft.
- **Systembereiche beim Systemstart/Medium-Wechsel prüfen**: Systembereiche (z.B. Bootsektoren) Ihres Computers sollten nicht von der Virenkontrolle ausgeschlossen werden. Sie können hier festlegen, ob Sie diese beim Systemstart überprüfen oder beim Medium-Wechsel (neue DVD o.ä.). Generell sollten Sie zumindest eine dieser beiden Funktionen aktiviert haben.
- **Auf Dialer / Spyware / Adware / Riskware prüfen**: Mit der G Data Software können Sie Ihr System auch auf Dialer und andere Schadprogramme (Spyware, Adware, Riskware) überprüfen. Hierbei handelt es sich z.B. um Programme, die unerwünschte teure Internetverbindungen aufbauen und in ihrem wirtschaftlichen Schadpotential dem Virus in nichts nachstehen. Spyware kann z.B. Ihr Surfverhalten oder sogar sämtliche Tastatureingaben (und damit auch Ihre Passwörter) unbemerkt speichern und bei nächster Gelegenheit übers Internet an fremde Personen weiterleiten.
- **Anwender bei Virenfund benachrichtigen**: Wird diese Option aktiviert, öffnet sich bei einem Virenfund durch den Wächter auf dem betroffenen Client ein Hinweisfenster, das den Anwender darüber in Kenntnis setzt, dass auf seinem System ein Virus gefunden wurde. Die gefundene Datei sowie der Pfad und die Bezeichnung des gefundenen Schädlings werden dort angezeigt.

Ausnahmen

Hier können Sie beim Client die Virenprüfung auch auf bestimmte Verzeichnisse begrenzen. Auf diese Weise können Sie z.B. Ordner mit selten benötigten Archiven aussparen, um diese in einem gesonderten Scanauftrag zu prüfen. Des Weiteren lassen sich bestimmte Dateien und Dateitypen von der Virenprüfung ausschließen. Folgende Ausnahmen sind möglich:

- **Laufwerk**: Wählen Sie hier mit Anklicken der Verzeichnis-Schaltfläche ein Laufwerk (Partition, Festplatte) aus, welches Sie vom Wächter nicht kontrollieren lassen möchten.
- **Verzeichnis**: Wählen Sie hier mit dem Anklicken der Verzeichnis-Schaltfläche einen Ordner (gegebenenfalls inkl. seiner darin befindlichen Unterordner) aus, der nicht vom Wächter kontrolliert werden soll.
- **Datei**: Hier können Sie den Namen der Datei eingeben, die Sie von der Wächterkontrolle ausnehmen möchten. Sie können hier auch mit Platzhaltern arbeiten.
- **Prozess**: Soll ein bestimmter Prozess nicht vom Wächter überwacht werden, ist der Name des betreffenden Prozesses hier einzutragen.

Sie können diesen Vorgang bei Bedarf beliebig oft wiederholen und im Wächter Ausnahmen-Fenster vorhandene Ausnahmen auch wieder löschen oder modifizieren.

> Die Funktionsweise von Platzhaltern ist folgendermaßen: Das Fragezeichen-Symbol (?) ist Stellvertreter für einzelne Zeichen. Das Sternchen-Symbol (*) ist Stellvertreter für ganze Zeichenfolgen. Um z.B. sämtliche Dateien mit der Dateiendung **exe** schützen zu lassen, geben Sie also ***.exe** ein. Um z.B. Dateien unterschiedlicher Tabellenkalkulationsformate zu schützen (z.B. **xlr**, **xls**), geben Sie einfach ***.xl?** ein. Um z.B. Dateien unterschiedlichen Typs mit einem anfänglich gleichen Dateinamen zu schützen, geben Sie beispielsweise **text*.*** ein. Dies würde die Dateien *text1.txt, text2.txt, text3.txt* usw. betreffen.

Verhaltensüberwachung

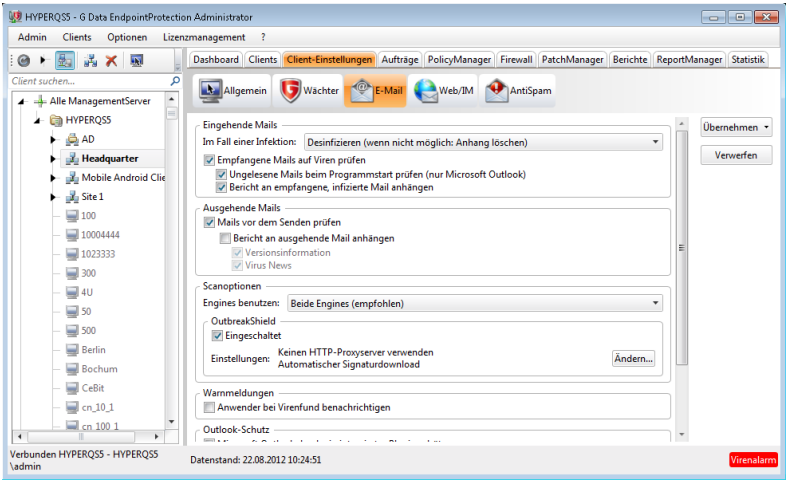
Die Verhaltensüberwachung stellt einen weiteren Schutz vor schädlichen Dateien und Prozessen dar, der im Unterschied zum Wächter, nicht signaturbasiert arbeitet, sondern das tatsächliche Verhalten eines Prozesses analysiert. Um eine Einordnung vorzunehmen, legt die Verhaltensüberwachung verschiedene Kriterien zugrunde, unter anderem Schreibzugriffe auf die Registry und das eventuelle Anlegen von Autostarteinträgen. Sind genügend Merkmale vorhanden, die den Schluss zulassen, dass ein Programm zumindest verdächtiges Verhalten an den Tag legt, wird die unter **Im Fall einer Bedrohung** eingestellte Aktion durchgeführt. Hierbei stehen die Optionen **Nur protokollieren**, **Programm anhalten** sowie **Programm anhalten und in Quarantäne verschieben** zur Verfügung. Bei der Einstellung **Nur protokollieren** wird das Programm nicht weiter beeinflusst und es wird nur unter **Berichte** eine entsprechende Meldung angezeigt.

Status

Hier wird Ihnen angezeigt, ob die am Wächter durchgeführten Änderungen schon für den Client oder die Gruppe übernommen wurden.

E-Mail

Auf jedem G Data Security Client kann ein gesonderter Virenschutz für E-Mails eingerichtet werden. Hierbei werden Standardports für die Protokolle POP3, IMAP und SMTP überwacht. Für Microsoft Outlook findet darüber hinaus ein spezielles Plug-In Verwendung. Das Plug-In überprüft automatisch alle eingehenden Mails auf Viren und verhindert, dass infizierte Mails versendet werden.



Eingehende Mails

- **Im Fall einer Infektion**: Hier können Sie festlegen, was bei Entdeckung einer infizierten Datei geschehen soll. Je nachdem, für welche Zwecke der jeweilige Client verwendet wird, sind hier unterschiedliche Einstellungen sinnvoll.
- **Empfangene Mails auf Viren prüfen**: Mit Aktivierung dieser Option werden sämtliche E-Mails auf Viren überprüft, die den Client online erreichen.
- **Ungelesene Mails beim Programmstart prüfen (nur für Microsoft Outlook)**: Diese Option dient dazu, E-Mails auf Virenbefall zu kontrollieren, die den Client erreichen, während dieser nicht mit dem Internet verbunden ist. Sobald Outlook geöffnet wird, werden deshalb sämtliche ungelesene Mails im Posteingang-Ordner und den darin enthaltenen Unterordnern kontrolliert.
- **Bericht an empfangene, infizierte Mails anhängen**: Sobald eine an den Client geschickte E-Mail einen Virus enthält, erhalten Sie im Body dieser Mail unter dem eigentlichen Mailtext die Meldung *ACHTUNG! Diese Mail enthält folgenden Virus* gefolgt vom Namen des Virus. Außerdem finden Sie vor dem eigentlichen Betreff die Mitteilung *[VIRUS]*. Sollten Sie die Option **Anhang/Text löschen** aktiviert haben, wird Ihnen außerdem mitgeteilt, dass der infizierte Teil der E-Mail gelöscht wurde.

Ausgehende Mails

- **Mails vor dem Senden prüfen**: Damit aus Ihrem Netzwerk keine Viren per Mail verschickt werden, bietet die G Data Software auch die Möglichkeit, Mails vor dem Versenden auf Virenbefall zu überprüfen. Sollte tatsächlich ein Virus versendet werden, erscheint die Meldung *Die Mail [Betreffzeile] enthält folgenden Virus: [Virusname]*. Die entsprechende E-Mail wird nicht versandt.
- **Bericht an ausgehende Mails anhängen**: Ein Prüfbericht wird im Body jeder ausgehenden E-Mail unter dem eigentlichen Mailtext angezeigt. Dieser lautet *Virengeprüft von G Data AntiVirus*, so lange Sie die Option **Mails vor dem Senden prüfen** aktiviert haben. Zusätzlich können Sie hier das Versionsdatum von G Data AntiVirus (**Versionsinformation**) angeben.

Scanoptionen

- **Engines benutzen**: Die G Data Software arbeitet mit zwei unabhängig voneinander operierenden Virenanalyseeinheiten, den so genannten Engines. Prinzipiell ist die Verwendung beider Engines der Garant für optimale Ergebnisse bei der Virenprophylaxe. Die Verwendung einer einzigen Engine bringt dagegen Performance-Vorteile mit sich; d.h. wenn Sie nur eine Engine verwenden, kann eine Analyse schneller durchgeführt werden.

- **OutbreakShield**: Mit dem OutbreakShield können Schädlinge in Massenmails schon erkannt und bekämpft werden, bevor aktualisierte Virensignaturen dafür verfügbar sind. Das OutbreakShield erfragt dabei über das Internet besondere Häufungen von verdächtigen Mails und schließt dabei in Echtzeit die Lücke, die zwischen dem Beginn eines Massenmailings und seiner Bekämpfung durch speziell angepasste Virensignaturen besteht. Unter **Ändern** können Sie festlegen, ob das OutbreakShield zur Steigerung der Erkennungsleistung zusätzliche Signaturen verwendet. Außerdem können Sie hier Zugangsdaten für die Internetverbindung oder einen Proxyserver eingeben, die dem OutbreakShield automatische Signaturdownloads aus dem Internet ermöglichen.

Warnmeldungen

- **Anwender bei Virenfund benachrichtigen**: Sie können den Empfänger einer infizierten Nachricht automatisch informieren. Auf seinem Desktop wird dann eine Virenmeldung angezeigt.

Outlook-Schutz

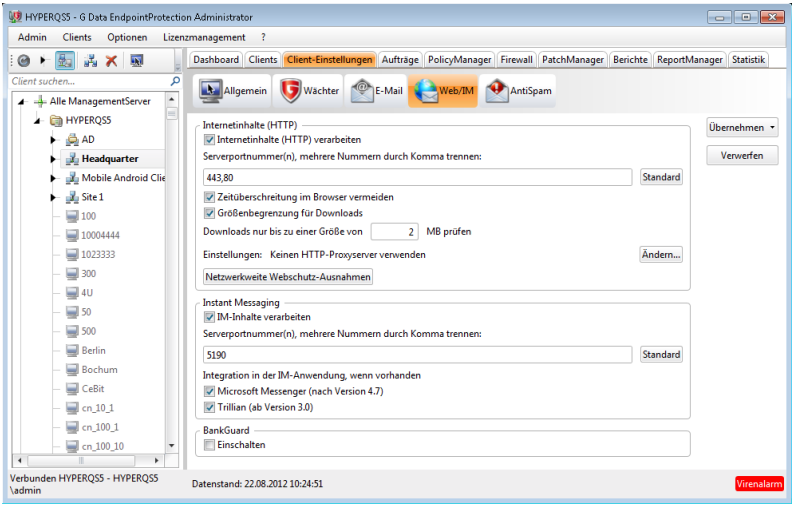
- **Microsoft Outlook durch ein integriertes Plug-In schützen**: Mit Aktivierung dieser Funktion wird in das Outlook des Clients im Menü **Extras** eine neue Funktion namens **Ordner auf Viren überprüfen** eingefügt. Unabhängig von den G Data Administrator-Einstellungen kann der Nutzer des einzelnen Clients den jeweils momentan ausgewählten Mailordner nach Viren durchsuchen. Im Ansichtsfenster einer E-Mail können Sie im Menü **Extras** über **Mail auf Viren überprüfen** eine Virenprüfung der Dateianlagen durchführen. Nach Abschluss des Vorgangs erscheint ein Info-Bildschirm, in dem das Ergebnis der Virenprüfung zusammengefasst wird. Hier erfahren Sie, ob die Virenanalyse vollständig erfolgte, erhalten Infos über die Anzahl der untersuchten Mails und Dateianhänge, etwaige Lesefehler sowie über gefundene Viren und wie damit verfahren wurde. Beide Fenster können Sie mit einem Klick auf die Schaltfläche **Schließen** ausblenden.

Port-Überwachung

Generell werden die Standardports für POP3 (110), IMAP (143) und SMTP (25) überwacht. Sollten die Porteinstellungen in Ihrem System davon abweichen, können Sie dies entsprechend anpassen.

Web/IM

In diesem Bereich können Sie Scan-Einstellungen für Internet, Instant Messaging und Online-Banking definieren. Wenn Sie die Internetinhalte nicht prüfen lassen wollen, greift der **Virenwächter** ein, wenn auf heruntergeladenen, infizierten Dateien zugegriffen wird. Das System auf dem jeweiligen Client ist also auch ohne die Überprüfung von Internetinhalten geschützt, solange der Virenwächter aktiviert ist.



Internetinhalte (HTTP)

- **Internetinhalte (HTTP) verarbeiten**: In den Web-Optionen können Sie bestimmen, dass sämtliche HTTP-Webinhalte schon beim Browsen auf Viren überprüft werden. Infizierte Webinhalte werden dann gar nicht erst ausgeführt und die entsprechenden Seiten nicht angezeigt. Wird im Netzwerk ein Proxy für den Zugang zum Internet genutzt, muss der Serverport eingetragen werden, den der Proxy nutzt. Sonst ist eine Überprüfung des Internetverkehrs nicht möglich. Auch die **Webinhaltskontrolle** (verfügbar in der G Data EndpointProtection) benutzt diese Einstellungen.
- **Zeitüberschreitung im Browser vermeiden**: Da die G Data Software die Webinhalte vor Ihrer Darstellung im Internet Browser bearbeitet und dafür je nach Datenaufkommen eine gewisse Zeit benötigt, kann es vorkommen, dass eine Fehlermeldung im Internet Browser erscheint, weil dieser nicht sofort die angeforderten Daten erhält, da diese zunächst von der Antivirensoftware auf Schadroutinen überprüft werden. Mit Setzen des Häkchens bei **Zeitüberschreitung im Browser vermeiden** wird diese Fehlermeldung unterdrückt. Sobald sämtliche Browserdaten auf Viren überprüft wurden, werden diese dann an den Internet Browser weitergereicht.

- **Größenbegrenzung für Downloads**: Hiermit können Sie die HTTP-Überprüfung für zu große Webinhalte aussetzen. Die Inhalte werden dann vom Virenwächter überprüft, sobald etwaige Schadroutinen aktiv werden. Der Vorteil bei dieser Größenbegrenzung liegt darin, dass es beim Download größerer Dateien nicht zu Verzögerungen durch die Virenkontrolle kommt.
- **Unternehmensweite Webschutz-Ausnahmen**: Diese Funktion erlaubt es Ihnen, bestimmte Webseiten generell von der Überprüfung durch den Webschutz auszunehmen.

Instant Messaging

- **IM-Inhalte verarbeiten**: Da auch über Instant Messaging-Programme Viren und andere Schadprogramme verbreitet werden, kann die G Data Software auch hier die Anzeige und den Download infizierter Daten im Vorfeld unterbinden. Sollten die verwendeten Instant Messaging-Anwendungen nicht die Standardports nutzen, geben Sie unter **Serverportnummer(n)**, die entsprechenden Ports ein.
- **Instant Messaging (Integration in der IM-Anwendung)**: Sollten Sie den Microsoft Messenger (ab Version 4.7) oder Trillian (ab Version 3.0) verwenden, steht durch Setzen des Häkchens für das jeweilige Programm ein Kontextmenü zur Verfügung, in dem Sie verdächtige Dateien direkt auf Viren überprüfen können.

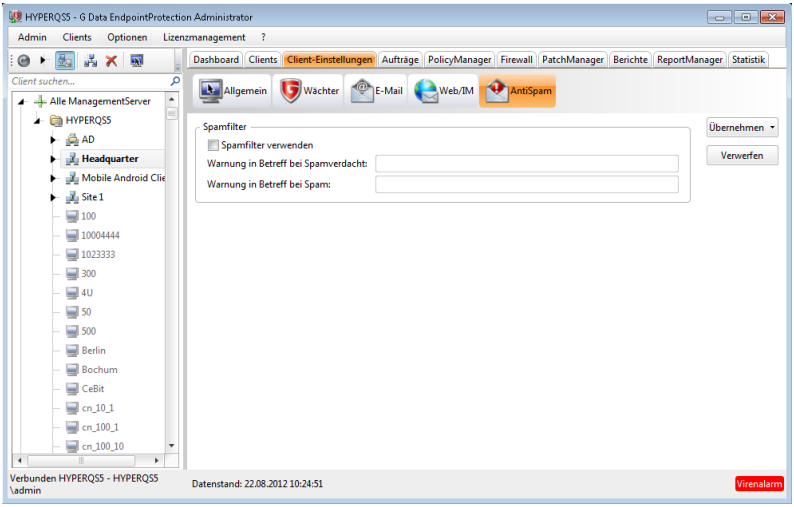
BankGuard

Banking-Trojaner werden zu einer immer größeren Bedrohung. Die wegweisende Technologie von G Data BankGuard sichert Bankgeschäfte von Anfang an und schützt sofort dort, wo der Angriff stattfindet. Durch eine Prüfung der Echtheit der benutzten Netzwerkbibliotheken stellt G Data BankGuard sicher, dass Internet-Browser nicht von einem Banking-Trojaner manipuliert werden. Durch diesen proaktiven Sofortschutz von mehr als 99 % sind Online-Bankgeschäfte bestmöglich geschützt - selbst vor bisher unbekannten Trojanern. BankGuard sollte für alle Clients aktiviert werden, die den Internet Explorer und/oder Firefox nutzen.

AntiSpam

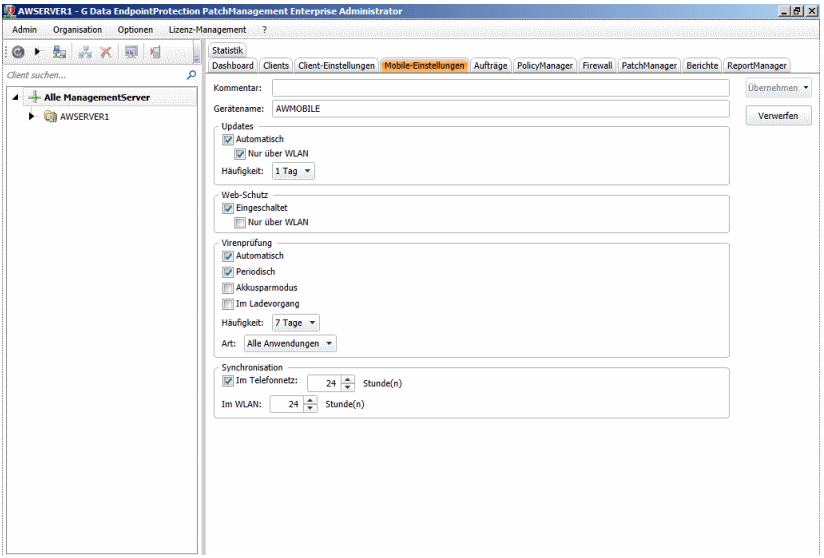
Wenn Sie das Häkchen bei **Spamfilter verwenden** setzen, wird der E-Mail-Verkehr des Clients auf eventuelle Spam-Mails überprüft. Sobald eine E-Mail als Spam erkannt wird oder unter Spamverdacht fällt, können Sie eine Warnung festlegen, die dann im Betreff der Mail angezeigt wird.

> Über die Warnung können Sie - oder der Anwender - auf dem Client im Mailprogramm eine Regel definieren, nach der z.B. Mails, die die Meldung *[Spam]* in der Betreffzeile haben, automatisch in einen speziellen Ordner für Spam- und Junk-Mail verschoben werden.



Mobile-Einstellungen

Wenn Sie einen mobilen Client im **Clientauswahlbereich** ausgewählt haben, können Sie hier die Einstellungen dafür ändern.



- **Kommentar**: Geben Sie hier ggf. ergänzende Informationen zum Client ein.
- **Gerätename:** Spezifizieren Sie hier anhand der Eingabe des Gerätenamens.

Updates

- **Automatisch**: Legen Sie hier fest, ob die Updates der Client-Software für Mobile Devices automatisch oder manuell erfolgen sollen. Falls sie sich für eine automatische Aktualisierung entscheiden, können Sie des Weiteren festlegen, wie oft dies zu erfolgen hat und ob eine Aktualisierung über das Mobilfunknetz oder nur über WLAN erfolgen soll.

Web-Schutz

- **Eingeschaltet**: Legen Sie hier fest, ob Mobile Devices beim Zugriff aufs Internet vom G Data Wächter geschützt werden sollen. Dies kann wahlweise als genereller Schutz eingestellt werden oder aber nur, wenn der Zugriff über WLAN erfolgen soll.

Virenprüfung

- **Automatisch**: Die Virenprüfung erfolgt automatisch und muss vom Anwender nicht manuell gestartet werden.
- **Periodisch**: Legen Sie hier fest, wie oft die Virenprüfung zu erfolgen hat, wenn diese automatisch ausgelöst wird. Sie können die Häufigkeit der Prüfung weiter unten einstellen. Hier können Sie außerdem einstellen, ob die Prüfung sich auf alle Anwendungen bezieht oder nur installierte Anwendungen.
- **Akkusparmodus**: Hier können Sie einen Virenscan erlauben oder unterbinden, wenn der Client im Akkusparmodus ist.
- **Im Ladevorgang**: Hier können Sie einen Virenscan erlauben oder unterbinden, wenn der Client sich im Ladevorgang befindet.
- **Art**: Hier können Sie festlegen, ob **Alle Anwendungen** gescannt werden sollen oder nur **Installierte Anwendungen**.

Synchronisation

Hier können Sie festlegen, ob und wie die Virensignaturen auf dem Mobile Device aktualisiert werden sollen. Geben Sie hier den Aktualisierungszyklus in Stunden an und entscheiden Sie, ob eine Synchronisation nur über WLAN oder auch über das Telefonnetz erfolgen soll.

Aufträge

In diesem Aufgabenbereich werden Aufträge auf den G Data Clients definiert. Es gibt zwei unterschiedliche Auftragsarten: Einmalige Aufträge und periodische Aufträge. Die einmaligen Jobs werden einmal zum festgelegten Zeitpunkt ausgeführt, für die periodischen wird ein Zeitplan definiert, nach dem sie ausgeführt werden sollen. Sie können beliebig viele unterschiedliche Aufträge definieren. Generell ist es aus Gründen der Performance allerdings sinnvoll, dass sich Aufträge zeitlich nicht überschneiden. Als Aufträge bzw. Jobs werden alle Aufträge bezeichnet, die am G Data ManagementServer erstellt werden. Es kann sich hier um Scanaufträge, Backup- oder Wiederherstellungsaufträge handeln.

Im Aufgabenbereich Aufträge erscheinen alle Jobs unter den von Ihnen vorgegebenen Namen und lassen sich durch einfaches Klicken auf die jeweilige Spaltenbezeichnung nach folgenden Kriterien sortieren. Die Spalte, nach der die aktuelle Sortierung erfolgt, wird dabei durch ein kleines Pfeilsymbol gekennzeichnet:

- **Name**: Der von Ihnen vorgegebene Name für den Job. Sie können hier beliebig lange Namen eingeben und auf diese Weise Ihren Job genau beschreiben, um bei vielen verschiedenen Jobs den Überblick zu behalten.
- **Client**: Hier finden Sie den Namen des jeweiligen Clients. Sie können Jobs nur für aktivierte Clients definieren.
- **Gruppe**: Sie können einzelne Clients zu Gruppen zusammenfassen, die dann dieselben Jobs nutzen. Wenn Sie einer Gruppe einen Job zuordnen, erscheinen in der Übersichtsliste nicht die einzelnen Rechner, sondern der Gruppenname.
- **Status**: Hier erhalten Sie den Status oder das Ergebnis eines Jobs im Klartext angezeigt. So erfahren Sie z.B., ob der Job gerade durchgeführt oder abgeschlossen wurde und werden auch darüber informiert, ob Viren gefunden wurden oder nicht.
- **Letzte Ausführung**: Über diese Spalte erhalten Sie Informationen darüber, wann der jeweilige Job das letzte Mal durchgeführt wurde.
- **Zeitintervall**: Gemäß der Zeitplanung, die Sie für jeden Job definieren können, steht hier, in welchem Turnus der Job wiederholt wird.
- **Umfang**: Hier erfahren Sie auf welche Datenträger (z.B. lokale Festplatten) sich die Analyse erstreckt.

Einstellungs- und Ansichtsoptionen

Aktualisieren: Diese Funktion aktualisiert die Ansicht und lädt die aktuelle Jobliste vom G Data ManagementServer.

Löschen: Die Funktion **Löschen...** löscht alle markierten Jobs.

Einmaliger Scanauftrag: Mit dieser Funktion lassen sich Scanaufträge für einzelne Rechner oder Rechnergruppen definieren. Im Konfigurationsdialog lassen sich auf den jeweiligen Karteireitern Analyseumfang und weitere Scaneinstellungen festlegen. Erfahren Sie mehr zu den Einstellungsmöglichkeiten für Scanaufträge im Kapitel **Scanaufträge definieren**. Wählen Sie zum Ändern der Scan-Parameter im Kontextmenü (über Anklicken mit der rechten Maustaste) den Befehl **Eigenschaften**. Nun können Sie die Einstellungen des Scanauftrags beliebig verändern.

Periodischer Scanauftrag: Mit dieser Funktion lassen sich Scanaufträge für einzelne Rechner oder Rechnergruppen definieren. Im Konfigurationsdialog lassen sich auf den jeweiligen Karteireitern Wiederholungsintervall, Analyseumfang und weitere Scaneinstellungen festlegen. Erfahren Sie mehr zu den Einstellungsmöglichkeiten für Scanaufträge im Kapitel **Scanaufträge definieren**. Wählen Sie zum Ändern der Scan-Parameter im Kontextmenü (über Anklicken mit der rechten Maustaste) den Befehl **Eigenschaften**. Nun können Sie die Einstellungen des Scanauftrags beliebig verändern.

Backup-Auftrag: Definieren Sie hier, wann und in welchem Umfang die Daten auf Clients gebackupt werden sollen. Erfahren Sie mehr zu den Einstellungsmöglichkeiten für Backupaufträge im Kapitel **Backupaufträge definieren**. Backup-Funktionalitäten stehen Ihnen nur in den **Enterprise-Versionen** der Software zur Verfügung.

Wiederherstellungsauftrag: Mit dieser Funktion lassen sich auf Clients oder Gruppen zentral Backups zurückspielen. Die Wiederherstellungsfunktion steht Ihnen nur in den **Enterprise-Versionen** der Software zur Verfügung.

Softwareerkennungsauftrag: Mit dieser Funktion lässt sich auf Clients oder Gruppen installierte Software ermitteln. Erfahren Sie mehr zu den Einstellungsmöglichkeiten für Softwareerkennungs-Aufträge im Kapitel **Softwareerkennung definieren**. Die Softwareerkennung steht Ihnen zur Verfügung, wenn Sie das optionale **PatchManagement-Modul** verwenden.

Softwareverteilungsauftrag: Mit dieser Funktion lässt sich auf Clients oder Gruppen installierte Software ermitteln. Erfahren Sie mehr zu den Einstellungsmöglichkeiten für Softwareerkennungs-Aufträge im Kapitel **Softwareverteilung definieren**. Die Softwareverteilung steht Ihnen zur Verfügung, wenn Sie das optionale **PatchManagement-Modul** verwenden.

Scanaufträge erneut (sofort) ausführen: Wählen Sie diese Funktion, um **einmalige Scanaufträge**, die bereits durchgeführt oder abgebrochen wurden, erneut auszuführen. Bei periodischen Scanaufträgen bewirkt diese Funktion, dass sie unabhängig vom Zeitplan sofort ausgeführt werden.

Protokolle: Rufen Sie mit dieser Funktion die Protokolle zu den Aufträgen des jeweiligen Clients auf.

Alle Aufträge anzeigen

Nur Scan-Aufträge anzeigen

Nur Backup-Aufträge anzeigen (diese Funktion steht Ihnen nur in den **Enterprise-Versionen** der Software zur Verfügung)

Nur Wiederherstellungsaufträge anzeigen (diese Funktion steht Ihnen nur in den **Enterprise-Versionen** der Software zur Verfügung)

Nur Softwareerkennungsaufträge anzeigen (diese Funktion steht Ihnen nur in Verbindung mit dem **PatchManagement-Modul** zur Verfügung)

Nur Softwareverteilungsaufträge anzeigen (diese Funktion steht Ihnen nur in Verbindung mit dem **PatchManagement-Modul** zur Verfügung)

Nur Rollbackaufträge anzeigen (diese Funktion steht Ihnen nur in Verbindung mit dem **PatchManagement-Modul** zur Verfügung)

Nur einmalige Scanaufträge anzeigen

Nur periodische Scanaufträge anzeigen

Nur offene Scanaufträge anzeigen

Nur erledigte Scanaufträge anzeigen

Gruppenjobs ausführlich anzeigen: Zeigt bei Gruppenjobs alle zugehörigen Einträge an. Die Option ist nur verfügbar, wenn in der Computerliste eine Gruppe selektiert ist.

Menüleiste

In der Menüleiste steht Ihnen für den Aufgabenbereich Aufträge ein zusätzlicher Menüeintrag mit folgenden Funktionen zur Verfügung:

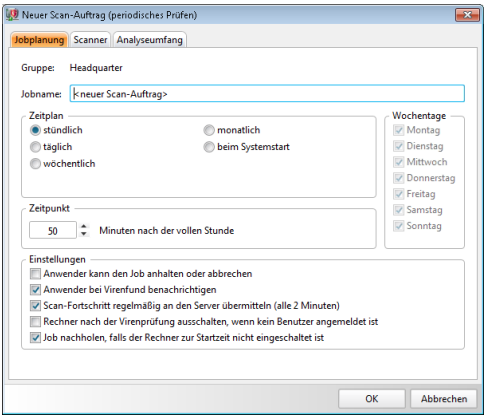
- **Ansicht**: Wählen Sie hier aus, ob Sie sich alle Aufträge anzeigen lassen möchten oder nur spezielle Vorgänge (z.B. Antivirenscan, Backup, Softwareerkennung, Softwareverteilung, Rollback usw. je nach installierter Software-Version). Für Scanaufträge, die für eine Gruppe von Clients definiert wurden, können Sie festlegen, ob detaillierte Infos zu allen Clients oder nur gruppenübergreifende Zusammenfassungen angezeigt werden sollen. Setzen Sie hierzu das Häkchen bei **Gruppenjobs ausführlich anzeigen**.

- **Sofort (erneut) ausführen**: Hiermit können Sie ausgewählte Jobs unabhängig von eingestellten zeitlichen Vorgaben direkt ausführen.
- **Abbrechen**: Über diese Funktion können Sie einen laufenden Job abbrechen.
- **Löschen**: Ausgewählte Jobs können mit dieser Funktion gelöscht werden.
- **Backup wiederherstellen**: Hiermit können Sie übers Netzwerk Backups auf den Clients einspielen.
- **Neu**: Wählen Sie hier aus, ob Sie eine einmalige Prüfung oder eine periodische Antivirenprüfung (Scan-Job) anlegen möchten. Hier können Sie darüber hinaus auch andere Vorgänge planen (z.B. Backup, Softwareerkennung, Softwareverteilung, Rollback usw. je nach installierter Software-Version).

Scanaufträge definieren

Jobplanung

Hier kann festgelegt werden, welchen Namen der Scanauftrag haben soll. Hier sollten aussagekräftige Namen, wie *Archivprüfung* oder *Monatliche Prüfung* Verwendung finden, um den gewünschten Job eindeutig zu charakterisieren und in der tabellarischen Übersicht wiederzufinden. Darüber hinaus können den Anwendern Berechtigungen zum Anhalten oder Abbrechen des Jobs über das Kontextmenü des Trays eingeräumt werden. Über die Option **Scan-Fortschritt regelmäßig an den Server übermitteln** können Sie sich im G Data Administrator den Fortschritt eines laufenden Scanauftrags auf einem Client in Prozent anzeigen lassen. Mit der Funktion **Rechner nach der Virenprüfung ausschalten, wenn kein Benutzer angemeldet ist** haben Sie eine weitere Option, die Ihnen hilft, den administrativen Aufwand zu verringern. Sollte ein Rechner zum festgelegten Zeitpunkt eines Scanauftrags nicht eingeschaltet sein, kann über die Option **Job nachholen, falls der Rechner zur Startzeit nicht eingeschaltet ist**, der Scanauftrag gestartet werden, wenn der Rechner nach diesem Zeitpunkt hochgefahren wird.



Bei einmaligen Scanaufträgen können Sie eine Startzeit definieren, bei periodischen Scanaufträgen können Sie festlegen, wann und in welchem Rhythmus die Virenprüfung erfolgen soll. Wird **Beim Systemstart** ausgewählt, fallen die Vorgaben der Zeitplanung weg und die G Data Software führt die Prüfung aus, wenn der Rechner neu gestartet wird. Unter **Täglich** können Sie mit Hilfe der Angaben unter **Wochentage** bestimmen, dass der Rechner nur an Werktagen eine Virenprüfung durchführt oder eben nur an jedem zweiten Tag oder gezielt an Wochenenden, an denen er nicht zur Arbeit genutzt wird.

> Wird ein einmaliger Scanauftrag angelegt, steht nur die Option **Startzeit verwenden** zur Verfügung. Ohne Angabe einer Startzeit wird der Scanauftrag sofort nach dem Anlegen gestartet.

Scanner

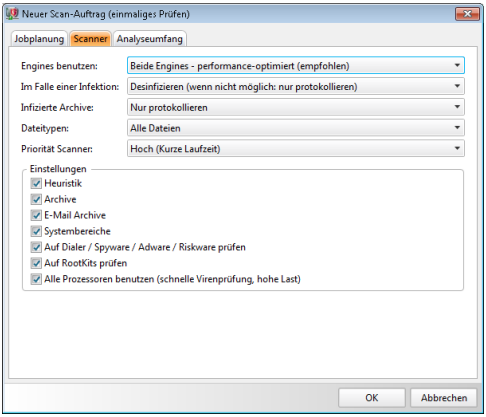
In dem Scanner-Menü lassen sich die Einstellungen vornehmen, mit denen der Scanauftrag ausgeführt werden soll. Die folgenden Optionen sind verfügbar:

- **Engines benutzen**: Die G Data Software arbeitet mit zwei unabhängig voneinander operierenden Virenanalyseeinheiten. Prinzipiell ist die Verwendung beider Engines der Garant für optimale Ergebnisse bei der Virenbekämpfung. Die Verwendung einer einzigen Engine bringt dagegen Performance-Vorteile mit sich; d.h. wenn Sie nur eine Engine verwenden, kann der Analysevorgang schneller erfolgen. Wir empfehlen die Einstellung **Beide Engines - performance-optimiert**. Hierbei sind beide Virenscanner so miteinander verwoben, dass sie die optimale Erkennung mit minimierter Scandauer ermöglichen.
- **Im Fall einer Infektion**: Hier können Sie festlegen, was bei Entdeckung einer infizierten Datei geschehen soll. Je nachdem, für welche Zwecke der jeweilige Clientrechner verwendet wird, sind hier unterschiedliche Einstellungen sinnvoll. Bei der Einstellung **Datei in Quarantäne verschieben** wird eine infizierte Datei in ein spezielles Verzeichnis verschoben, welches der G Data ManagementServer anlegt. Dort werden infizierte Dateien verschlüsselt, sodass etwaige Schadfunktionen nicht mehr ausgeführt werden können. Dateien in der Quarantäne können vom Netzwerkadministrator desinfiziert, gelöscht, an den Ursprungsort zurückbewegt oder gegebenenfalls an die **Internet-Ambulanz** gesandt werden.
- **Infizierte Archive**: Legen Sie hier fest, wie infizierte **Archive** behandelt werden sollen. Beachten Sie beim Festlegen dieser Einstellungen, dass ein Virus innerhalb eines Archives erst dann Schaden anrichtet, wenn das Archiv entpackt wird.
- **Dateitypen**: Hier können Sie festlegen, welche Dateitypen von G Data auf Viren untersucht werden sollen. Beachten Sie, dass eine Überprüfung aller Dateien eines Computers eine gewisse Zeit in Anspruch nehmen kann.

- **Priorität Scanner**: Über die Stufen **hoch**, **mittel** und **niedrig** können Sie festlegen, ob eine Virenprüfung durch G Data auf Ihrem System hohe Priorität haben soll (in diesem Fall erfolgt die Analyse schneller, allerdings sind Performanceeinbußen bei anderen Anwendungen möglich) oder niedrige Priorität (die Analyse benötigt mehr Zeit, dafür werden andere Anwendungen nicht beeinträchtigt). Je nach der Zeit, zu der Sie die Virenanalyse durchführen, sind hier unterschiedliche Einstellungen sinnvoll.
- **Einstellungen**: Legen Sie hier fest, welche zusätzlichen Virenanalysen die G Data Software durchführen soll. Die hier gewählten Optionen sind für sich gesehen durchaus sinnvoll, je nach Anwendungsart kann der Vorteil der Zeitersparnis durch Weglassen dieser Überprüfungen das etwas geringere Maß an Sicherheit aufwiegen. Folgende Einstellungsmöglichkeiten stehen Ihnen hier zur Verfügung:

  - **Heuristik**: In der Heuristik werden Viren nicht nur anhand der Virendatenbanken, sondern auch anhand bestimmter virentypischer Merkmale ermittelt. Die Heuristik kann in sehr seltenen Fällen einen Fehlalarm erzeugen.
  - **Archive**: Das Überprüfen gepackter Daten in Archiven ist sehr zeitintensiv und kann in der Regel unterbleiben, wenn der **G Data Wächter** auf dem System aktiv ist. Dieser erkennt dann beim Entpacken des Archives einen bis dahin verborgenen Virus und unterbindet automatisch dessen Verbreitung. Dennoch sollten bei regelmäßigen Kontrollen, außerhalb der eigentlichen Nutzungszeit des Computers, auch eine Prüfung der Archive erfolgen.
  - **E-Mail Archive**: Das Überprüfen von E-Mail Archiven ist sehr zeitintensiv und kann in der Regel unterbleiben, wenn der **G Data Wächter** bzw. das Outlook-Plugin auf dem System aktiv ist. Der Wächter erkennt beim Zugriff auf das Archiv einen bis dato verborgenen Virus und unterbindet automatisch dessen Verbreitung. Dennoch sollten bei regelmäßigen Kontrollen, außerhalb der eigentlichen Nutzungszeit des Computers, auch eine Kontrolle der Archive erfolgen.
  - **Systembereiche**: Die Systembereiche Ihres Computers (Bootsektoren, Master Boot Record etc.) die eine grundlegende Basis für das Betriebssystem bieten, sollten nicht von der Virenkontrolle ausgeschlossen werden, da sich einige Schädlinge speziell in diesem Bereich des Systems einnisten können.
  - **Auf Dialer / Spyware / Adware / Riskware prüfen**: Mit der G Data Software können Sie Ihr System auch auf Dialer und andere Schadprogramme (Spyware, Adware, Riskware) überprüfen. Hierbei handelt es sich z.B. um Programme, die unerwünschte teure Internetverbindungen aufbauen und in ihrem wirtschaftlichen Schadpotential dem Virus in nichts nachstehen. Spyware kann z.B. Ihr Surfverhalten oder sogar sämtliche Tastatureingaben (und damit auch Ihre Passwörter) unbemerkt speichern und bei nächster Gelegenheit über das Internet an fremde Personen weiterleiten.

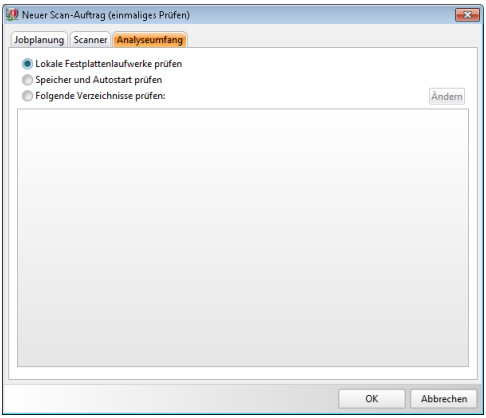
- **Auf RootKits prüfen**: Ein Rootkit versucht, sich herkömmlichen Virenerkennungsmethoden zu entziehen. Sie können mit dieser Funktion gezielt nach Rootkits suchen, ohne eine komplette Überprüfung der Festplatten und gespeicherten Daten vorzunehmen.
- **Alle Prozessoren benutzen**: Mit dieser Option können Sie die Virenprüfung bei Systemen mit mehreren Prozessorkernen auf alle Prozessoren verteilen und auf diese Weise die Virenprüfung deutlich schneller durchführen. Nachteil dieser Option ist, dass so weniger Rechenleistung für andere Anwendungen verfügbar ist. Diese Option sollte nur dann genutzt werden, wenn der Scanauftrag zu Zeiten durchgeführt werden, zu denen das System nicht regulär genutzt wird (z.B. nachts).



Analyse-Umfang

Über das Register **Analyse-Umfang** lässt sich beim Client die Virenkontrolle auch auf bestimmte Verzeichnisse begrenzen. Auf diese Weise können z.B. Ordner mit selten benötigten Archiven ausgespart und in einem separaten Scanauftrag geprüft werden. Das Verzeichnisauswahl-Fenster erlaubt Ihnen Ordner auf Ihrem Rechner und im Netzwerk auszuwählen.

> Besonderheit bei Scanaufträgen auf einem Linux-Fileserver: Bei der Verzeichnisauswahl werden das Root-Laufwerk (/) und alle Freigaben zurück geliefert. So können Scanaufträge gezielt auf ausgewählten Freigaben oder beliebig gewählten Verzeichnissen des Dateiservers durchgeführt werden.



Backupaufträge definieren

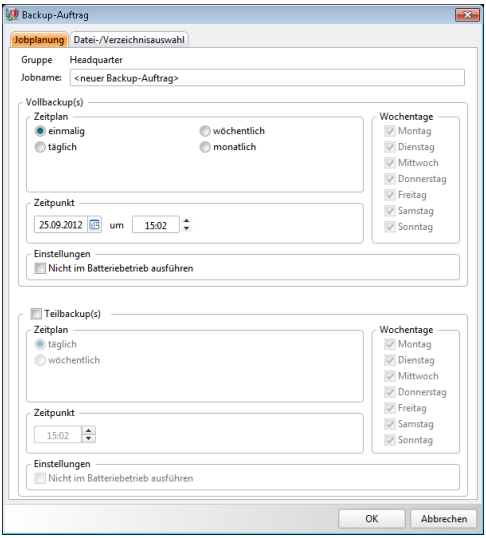
Die Backup-Funktion steht Ihnen nur als Teil der **Enterprise** Software-Versionen zur Verfügung.

Jobplanung

Hier kann festgelegt werden, welchen Namen der Backupauftrag haben soll. Hier sollten aussagekräftige Namen, wie *Monatsbackup* oder *Teilbackup Außendienst* Verwendung finden, um den gewünschten Job eindeutig zu charakterisieren und in der tabellarischen Übersicht wiederzufinden. Sie können hier festlegen, wann und in welchem Rhythmus das Backup erfolgen soll und ob es sich dabei um ein **Teilbackup** oder **Vollbackup** handelt. Beim Teilbackup werden nur die Daten gebackupt, die sich seit dem letzten Teil- oder Vollbackup geändert haben. Dies spart Zeit bei der Erstellung des Backups, die Wiederherstellung ist im Fall eines Zurückspielens von Daten allerdings langwieriger, da aus den verschiedenen Teilbackupdatenbeständen das letzte Systemabbild rekonstruiert werden muss.

Um Probleme zu vermeiden, die sich beim Abschalten eines nicht ans Stromnetz angeschlossenen Notebooks ergeben, können Sie die Einstellung **Nicht im Batteriebetrieb ausführen** auswählen. Backups von mobilen Geräten erfolgen dann nur, wenn diese auch ans Stromnetz angeschlossen sind. Unter **Täglich** können Sie mit Hilfe der Angaben unter **Wochentage** bestimmen, dass der Rechner nur an Werktagen eine Backup durchführt oder eben nur an jedem zweiten Tag oder gezielt an Wochenenden, an denen er nicht zur Arbeit genutzt wird.

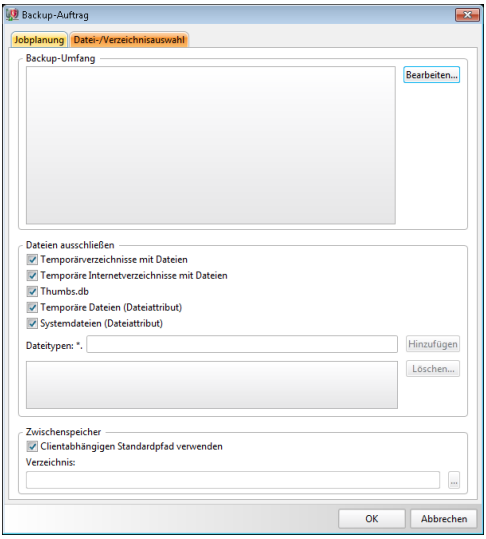
Sofern nichts anderes in den **Server-Einstellungen** angegeben ist, werden die Backups vom ManagementServer im Verzeichnis **C:\ProgramData\G DATA\AntiVirus ManagementServer\Backup** oder **C:\Documents and Settings\All Users \Application Data\G DATA\AntiVirus ManagementServer\Backup** gespeichert. Wenn nicht genügend Speicherplatz auf dem Client verfügbar ist, wenn das Backup durchgeführt wird, erscheint eine entsprechende Fehlermeldung im G Data Administrator.



Datei-/Verzeichnisauswahl

Über die Registerkarte **Datei-/Verzeichnisauswahl** können Sie festlegen, welchen Daten genau bei den einzelnen Clients/Gruppen vom Backup erfasst werden sollen. Im Bereich **Backup-Umfang** können Sie dazu direkt im Verzeichnisbaum des jeweiligen Clients die Ordner festlegen, die gesichert werden sollen. Über die Häkchen unter **Dateien ausschließen** können Sie generell Dateien und Ordner mit bestimmten Attributen (z.B. temporäre Ordner und Dateien, Systemdateien) vom Backup ausschließen, Darüber hinaus können Sie auch individuelle Ausnahmen definieren, indem Sie die Endung bestimmter Dateitypen auf die Ausnahmeliste setzen.

Wenn die erstellte Sicherung in einem bestimmten Verzeichnis gespeichert werden soll, bevor Sie an den ManagementServer übermeittelt wird, können Sie dies unter **Zwischenspeicher** explizit angeben. Wenn Sie die Option **Clientabhängigen Standardpfad verwenden** auswählen und ein absoluter Pfad angegeben ist, wird die Sicherung in dem angegebenen Verzeichnis zwischengespeichert. Wenn die Option nicht aktiv ist, wird der G Data Client das Backup immer auf der Partition durchführen, auf der der meiste freie Speicherplatz vorhanden ist. Das Verzeichnis **G Data\Backup** wird dann im Root-Verzeichnis dieser Partition angelegt.

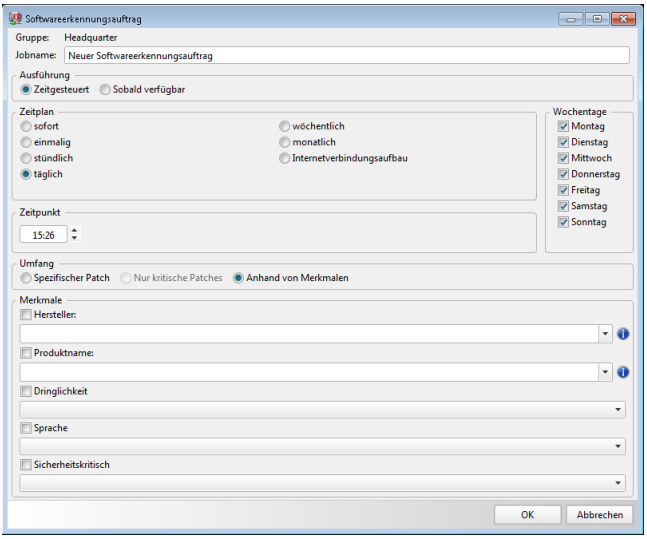


Softwareerkennung definieren

Die Softwareerkennung steht Ihnen nur zur Verfügung, wenn Sie das optionale **PatchManagement-Modul** installiert haben.

Mit dieser Funktion lässt sich auf Clients oder Gruppen die Anwendbarkeit von verfügbaren **Patches** ermitteln. Die Ausführung der Softwareerkennung kann dabei **zeitgesteuert** oder **sobald verfügbar** erfolgen. Wählen Sie aus, ob Sie die Anwendbarkeit von Software-Patches anhand von Merkmalen ermitteln möchten oder gezielt nach spezifischen Patches oder nur kritischen Patches suchen.

Geben Sie die Merkmale der Software an, die Sie erkennen möchten. Um bestimmte Merkmale (Hersteller, Produktname, Dringlichkeit, Sprache) als Auswahlkriterium zuzulassen, setzen Sie bitte das Häkchen beim jeweiligen Merkmal. So können Sie z.B. Software nur von bestimmten Herstellern ermitteln oder konkrete Programmversionen einer Software. Wildcards wie "?" und "*" zur Filterung sind dabei zulässig.

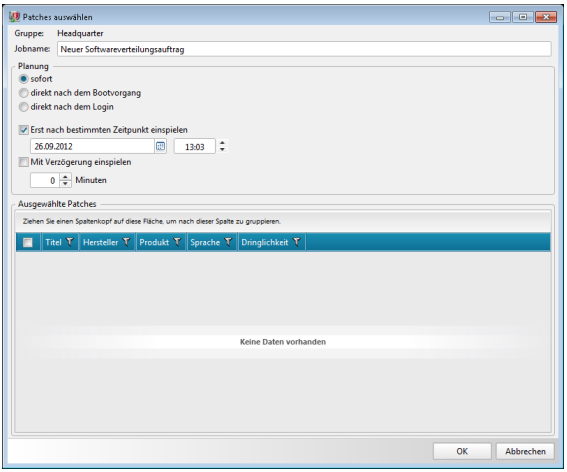


Softwareverteilung definieren

Die SoftwareVerteilung steht Ihnen nur zur Verfügung, wenn Sie das optionale **PatchManagement-Modul** installiert haben.

Hier können Sie festlegen wann **ausgewählte Patches**, die anwendbar sind, auf den Clients und Gruppen installiert werden sollen. Durch Auswahl der Option **Erst nach bestimmten Zeitpunkt einspielen** können Sie den Job zeitlich planen. Dabei können Sie wählen zwischen: **sofort**, **direkt nach dem Bootvorgang**, oder **direkt nach dem Login**. Über die Einstellung bei **Mit Verzögerung einspielen** können Sie das Einspielen von Patches zeitlich vom Bootvorgang trennen. Vorteil hierbei: Bootvorgang und Patcheinspielung beeinträchtigen nicht beide gleichzeitig die Performance des Clients.

Um bereits eingespielte Patches zu deinstallieren können Sie einen Rollback-Vorgang über den **Patch Manager** durchführen oder direkt per Rechtsklick in der Aufgabenliste auf den jeweiligen Distributionsjob durch Auswahl der Funktion **Rollback**.



PolicyManager

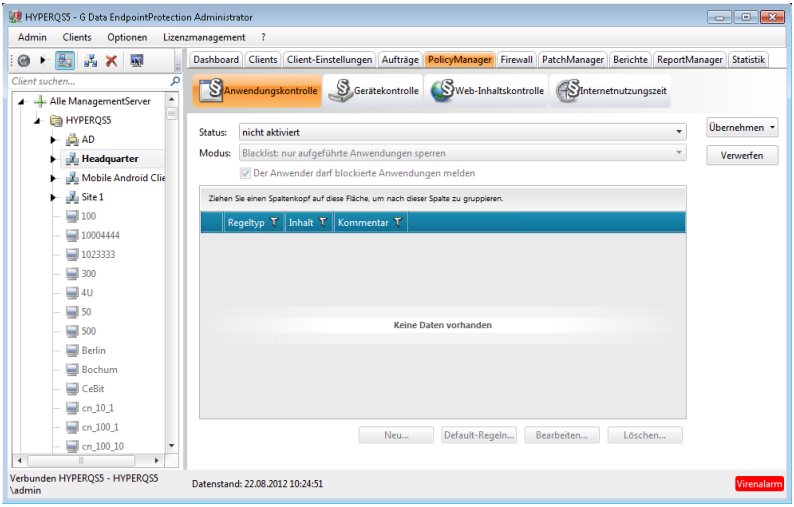
Das Modul **PolicyManager** steht Ihnen nur als Teil der Software-Versionen EndpointProtection Enterprise und EndpointProtection zur **Verfügung**.

Der PolicyManager enthält eine Anwendungs-, Geräte-, Web-Inhaltskontrolle sowie eine Überwachung der Internetnutzungeszeit. Diese Funktionen erlauben eine flächendeckende Umsetzung der Unternehmensrichtlinien zur Nutzung der firmeneigenen PCs. So kann über den PolicyManager bestimmt werden, ob und in welchem Umfang externe Massenspeicher- oder optische Medien genutzt werden können. Ebenso lässt sich definieren, welche Webseiten innerhalb welches Zeitrahmens besucht und welche Programme auf den Firmen-PCs genutzt werden dürfen.

Anwendungskontrolle

Mit der Anwendungskontrolle lassen sich bestimmte Programme für die Nutzung durch ausgewählte Clients sperren. Legen Sie dazu unter **Status** fest, ob die Einschränkungen für alle Benutzer des jeweiligen Clients gelten sollen oder nur für Benutzer, die keine Administratorberechtigungen auf dem Client-Rechner besitzen. Unter Modus bestimmen Sie nun, ob es sich bei der Anwendungskontrollliste um eine Whitelist oder Blacklist handeln soll.

- **Whitelist**: Nur die hier aufgeführten Anwendungen können vom Client-Rechner aus verwendet werden.
- **Blacklist**: Hier aufgeführte Anwendungen können auf dem Client-Rechner nicht verwendet werden.



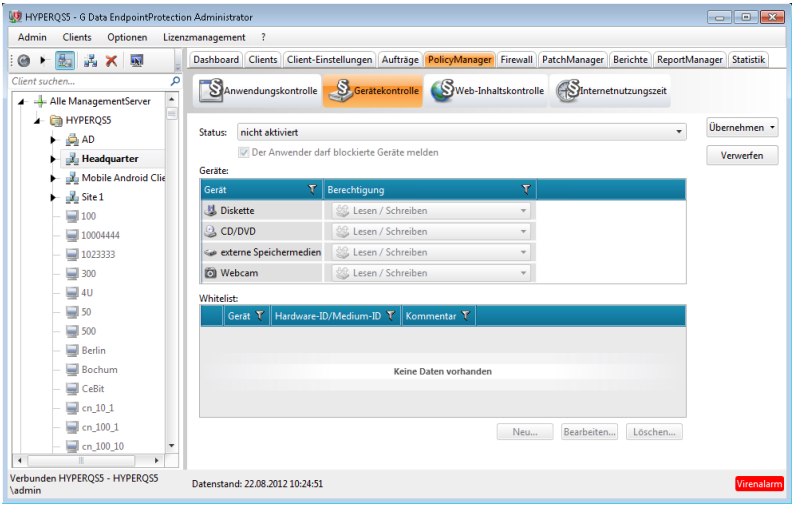
Neue Regel erstellen

Über die **Neu...**-Schaltfläche, kann eine neue Regel erstellt werden. Zur Auswahl stehen die Regeltpyen **Hersteller**, **Datei** und **Verzeichnis**.

- **Hersteller**: Hier werden die Herstellerinformationen in Programmdateien dazu verwendet, eine Nutzung dieser Anwendungen zu erlauben oder zu verbieten. Sie können den Namen des Herstellers hier entweder selbst eintragen oder über die **Hersteller suchen...** - Schaltfläche gezielt eine Datei auswählen, aus der die Herstellerinformation ausgelesen und übernommen wird.
- **Datei**: Hier können Sie bestimmte Programmdateien für den jeweiligen Client sperren oder erlauben. Dabei können Sie entweder den Dateinamen eingeben, um den Zugriff auf Dateien dieses Namens generell zu verbieten/zu erlauben oder Sie klicken auf die Schaltfläche **Merkmale einer Datei ermitteln...**, um ganz speziell eine bestimmte Datei anhand ihrer Merkmale zu definieren. Bei Bedarf können Sie als Platzhalter für beliebige Inhalte einen Stern (*) am Anfang und/oder Ende der Merkmale Dateiname, Produktname und Copyright verwenden.
- **Verzeichnis**: Über diese Funktion können Sie komplette Verzeichnisse (auf Wunsch inklusive der jeweiligen Unterverzeichnisse) für Clients freigeben oder sperren.

Gerätekontrolle

Mit Hilfe der Gerätekontrolle lässt sich der Zugriff auf externe Speichermedien begrenzen. So können USB-Sticks von der Nutzung ausgeschlossen, CD/DVD-Laufwerke mit Schreib- oder Leserechten ausgestattet und auch die Verwendung von Kameras eingeschränkt werden.



Unter **Status** können Sie festlegen, ob die Einschränkungen für alle Benutzer des jeweiligen Clients gelten sollen oder nur für Benutzer, die keine Administratorberechtigungen auf dem Client-Rechner besitzen. Für jeden Client werden unter **Geräte** die Geräteklassen angezeigt, deren Nutzung eingeschränkt werden kann. Diese müssen nicht zwangsläufig auch am jeweiligen Client vorhanden sein. So können zum Beispiel für ausgewählte Nutzergruppen generell die Nutzung von Diskettenlaufwerken untersagt werden, unabhängig davon, ob die jeweiligen Rechner ein Diskettenlaufwerk besitzen oder nicht. Folgende Berechtigungen lassen sich definieren:

- **Lesen / Schreiben**: Es besteht voller Zugriff auf das Gerät.
- **Lesen**: Medien können nur gelesen werden, ein Abspeichern von Daten ist nicht erlaubt.
- **Zugriff verbieten**: Sowohl Lese- als auch Schreibzugriffe auf das Gerät sind nicht erlaubt. Das Gerät kann vom Anwender nicht verwendet werden.

Whitelist

Über die Whitelist-Einstellungen können Sie die Gerätenutzung, die Sie für den Client-Nutzer in irgendeiner Weise eingeschränkt haben (**Lesen** / **Zugriff verbieten**) mit bestimmten Einschränkungen wieder erlauben. Wenn Sie auf die **Neu...**-Schaltfläche klicken, öffnet sich ein Dialogfenster, in dem die Geräte mit Nutzungseinschränkungen angezeigt werden. Wenn Sie nun auf **[...]** klicken, können Sie für bestimmte Geräte eine Ausnahme zulassen.

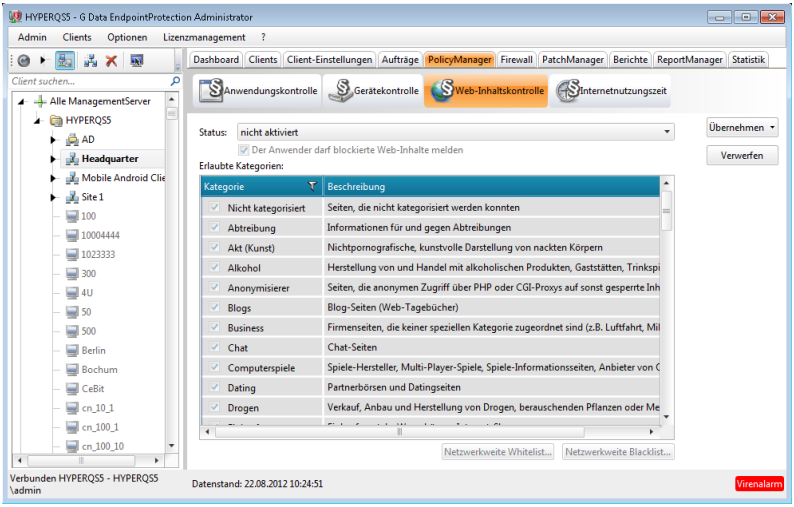
- **Medium-ID verwenden**: Hier können Sie z.B. festlegen, dass nur bestimmte CDs oder DVDs mit einem CD/DVD-Laufwerk genutzt werden können (z.B. spezielle Firmen-Präsentationen auf CD).
- **Hardware-ID verwenden**: Hier können Sie z.B. festlegen, dass nur bestimmte USB-Sticks verwendet werden dürfen. Bei Hardware-ID-basierten Freigaben für einzelne Speichergeräte hat der Netzwerkadministrator die Möglichkeit, zu kontrollieren, welche Mitarbeiter die Möglichkeit zur Weitergabe von Daten haben.

Um eine Medium-ID oder Hardware-ID zu ermitteln, klicken Sie im Dialogfeld **Hardware-ID/Medium-ID ermitteln** auf den Eintrag **Client** und wählen dort den Client aus, auf dem sich das freizugebende Medium befindet. Die entsprechende ID wird dann automatisch ausgelesen. Über die lokale Suche können Sie die ID des Mediums oder der Hardware mit Hilfe des Rechners ermitteln, auf dem der G Data Administrator installiert ist. Das Medium muss dazu an die entsprechende Maschine angeschlossen bzw. dort eingelegt sein.

Web-Inhaltskontrolle

Die Web-Inhaltskontrolle dient dazu, Anwendern zwar den dienstlichen Zugang zum Internet zu erlauben, aber das Surfen auf nicht erwünschten Websites oder in bestimmten Themenbereichen zu unterbinden. Sie können hier gezielt Bereiche durch Setzen eines Häkchens für den jeweiligen Client erlauben oder durch Entfernen des Häkchens verbieten. Die Kategorien decken dabei eine große Anzahl thematischer Bereiche ab und werden von G Data laufend aktualisiert. Somit entfällt für den Netzwerkadministrator der mit der Pflege von White- und Blacklists verbundene Aufwand.

Unter **Status** können Sie festlegen, ob die Einschränkungen für alle Benutzer des jeweiligen Clients gelten sollen oder nur für Benutzer, die keine Administratorenrechte auf dem Client-Rechner besitzen.



Netzwerkweite Whitelist

Mit der **netzwerkweiten Whitelist** können unabhängig von den Einstellungen, die unter **Erlaubte Kategorien** vorgenommen wurden, bestimmte Webseiten unternehmensweit für das gesamte Netzwerk freigegeben werden. Dies kann z.B. die Webpräsenz Ihres Unternehmens sein. Geben Sie dazu unter **URLs** die Adresse ein, die freigegeben werden soll, klicken Sie dann auf die Schaltfläche **Hinzufügen** und die entsprechede Seite ist freigegeben.

Netzwerkweite Blacklist

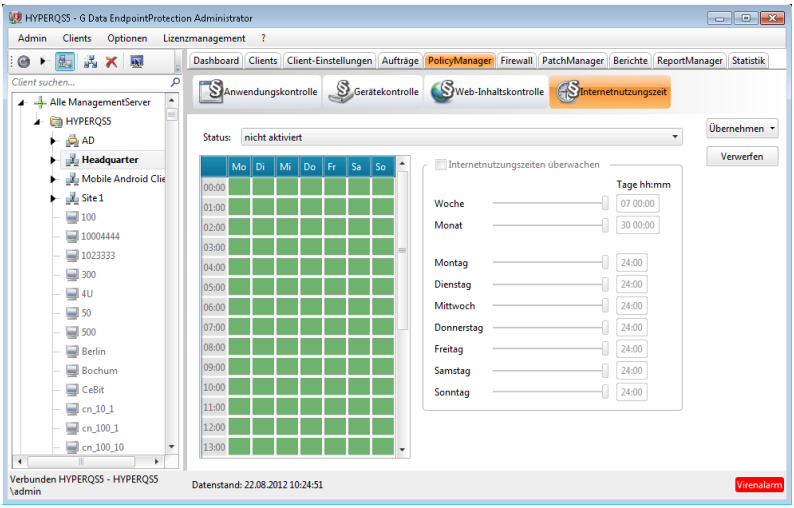
Mit der **netzwerkweiten Blacklist** können unabhängig von den Einstellungen, die unter **Erlaubte Kategorien** vorgenommen wurden, bestimmte Webseiten unternehmensweit für das gesamte Netzwerk gesperrt werden. Geben Sie dazu unter **URLs** die Adresse ein, die gesperrt werden soll, klicken Sie dann auf die Schaltfläche **Hinzufügen** und die entsprechede Seite ist gesperrt.

Internetnutzungszeit

Im Bereich Internetnutzungszeit kann die generelle Nutzung des Internets auf bestimmte Zeiten beschränkt werden. Zudem ist auch die Einrichtung eines Zeitkontingents für die Internetnutzung möglich. Unter **Status** wird festgelegt, ob die Einschränkungen für alle Benutzer des jeweiligen Clients gelten sollen oder nur für Benutzer, die keine Administratorberechtigungen auf dem Client-Rechner besitzen. Auf der rechten Seite kann über die dort vorhandenen Schieberegler das Kontingent festgelegt werden, dass auf dem jeweiligen Clientrechner für die Nutzung des Internets zur Verfügung steht. Es können tägliche, wöchentliche oder monatliche Kontingente vergeben werden; beispielsweise entspricht die Angabe **04/20:05** einer Internetnutzungszeit von 4 Tagen, 20 Stunden und 5 Minuten.

> Im Zusammenspiel der Angaben zur Internetnutzung zählt immer der jeweils kleinste Wert. Wenn Sie also für den Monat eine zeitliche Beschränkung von vier Tagen festlegen, in der Woche aber z.B. fünf Tage erlauben, deckelt die Software die Internetnutzung für den Benutzer automatisch auf vier Tage.

Wenn der jeweilige Benutzer versucht, über das erlaubte Zeitkontingent hinaus auf das Internet zuzugreifen, erscheint im Browser ein Info-Bildschirm, der ihn darüber informiert, dass er sein Zeitkontingent überschritten hat. Im Bereich Sperrzeiten können Sie - zusätzlich zur zeitlichen Eingrenzung der Internetnutzung - bestimmte Zeiträume sperren. Gesperrte Zeiträume sind dabei rot dargestellt, freigegebene Zeiträume in grün. Um einen Zeitraum freizugeben oder zu sperren, markieren Sie diesen mit der Maus. Dann erscheint neben dem Mauszeiger ein Kontextmenü, in dem Sie zwei Möglichkeiten haben: **Zeit freigeben** und **Zeit sperren**. Wenn der jeweilige Benutzer versucht, während der gesperrten Zeiten auf das Internet zuzugreifen, erscheint im Browser ein Info-Bildschirm, der ihn darüber informiert, dass er zu diesem Zeitpunkt keinen Zugriff auf das Internet hat.



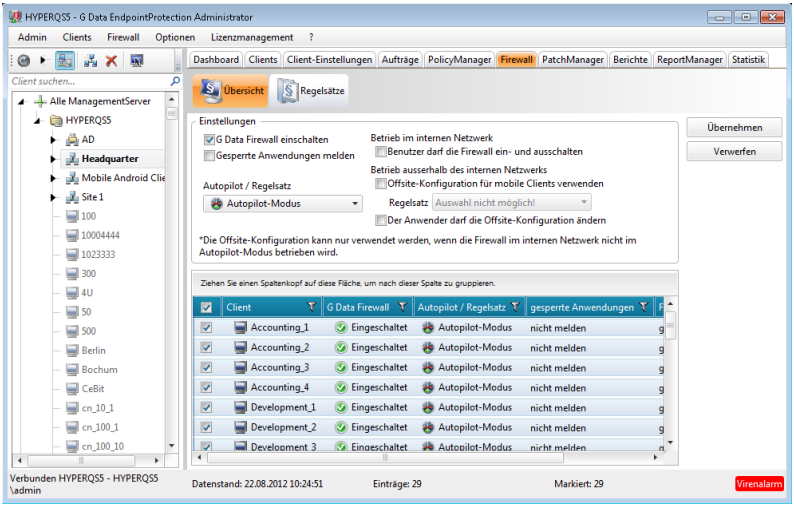
Firewall

Das Firewall-Modul steht Ihnen nur in den Software-Versionen ClientSecurity (Enterprise/Business) und EndpointProtection (Enterprise/Business) zur **Verfügung**.

In diesem Bereich kann die Firewall auf den jeweiligen Clients oder Gruppen zentral administriert werden. **Übersicht** gibt dem Systemadministrator eine Übersicht über den aktuellen Status der Firewall auf den installierten Clients, **Regelsätze** bietet Möglichkeiten zum Erstellen und Verwalten von Regelsätzen.

Übersicht

Es gibt zwei grundsätzlich verschiedene Möglichkeiten, eine Firewall zu betreiben. Wenn die Firewall auf **Autopilot** betrieben wird, ist sie schon standardmäßig von G Data vorkonfiguriert, erfüllt Ihre Aufgabe im Hintergrund und stört den Anwender nicht mit Rückfragen. Im Autopilotmodus optimiert die Firewall ihren Regelsatz mit der Zeit selbstständig. Als Administrator können Sie auch individuelle Firewallregeln für unterschiedliche Rechner definieren (**Regelsätze**).



In der Übersicht werden alle Client-Rechner oder die Clients einer ausgewählten Gruppe angezeigt. Hier sehen Sie auf einen Blick, welche Einstellungen die jeweilige Client-Firewall hat und können durch Anklicken des jeweiligen Clients direkt Änderungen vornehmen. Folgende Informationen hält die Übersichtsliste bereit:

- **Client**: Der Name des Client-Rechners. Anhand des abgebildeten Symbols können Sie hier erkennen, ob die Client-Software auf diesem Client installiert ist.
- **G Data Firewall**: Hier erfahren Sie, ob die Firewall auf dem Client eingeschaltet, ausgeschaltet oder ggf. gar nicht installiert ist.
- **Autopilot / Regelsatz**: Zeigt an, welcher Regelsatz für welchen Client angewendet wird.
- **Gesperrte Anwendungen**: Zeigt, ob blockierte Anwendungen bei Nutzungsaufruf gemeldet werden oder nicht.
- **Client Firewall**: Hier sehen Sie, ob der Client-Benutzer die Firewall aktivieren bzw. deaktivieren kann.

- **Offsite-Konfiguration**: Wenn Sie für einen Client die Offsite-Konfiguration auswählen, kann der Anwender auf diesem Client seine Firewall-Einstellungen individuell verwalten und einstellen, solange er nicht mit dem Netzwerk des G Data ManagementServers verbunden ist. Die Offsite-Konfiguration kann nur verwendet werden, wenn die Firewall im Firmennetz nicht im Autopilot-Modus betrieben wird.

Um die Firewall-Einstellungen für die in der Liste ausgewählten Clients zu ändern, klicken Sie den Eintrag mit der rechten Maustaste an. Es öffnet sich ein Auswahlmenü mit folgenden Optionen:

- **Regelsatz erstellen**: Hiermit wechseln Sie in den Bereich **Regelsätze** und können individuelle Regeln für ihre Client-Firewalls definieren.
- **Regelsatz bearbeiten**: Hiermit wechseln Sie in den Bereich Regelsätze und können bestehende Regeln für ihre Client-Firewalls ändern.
- **Firewall installieren**: Über diese Funktion können Sie auf aktivierten Client-Rechnern zentral eine Firewall installieren und im Anschluss administrieren.
- **Firewall deinstallieren**: Mit dieser Funktion wird die bestehende Client-Firewall deinstalliert.

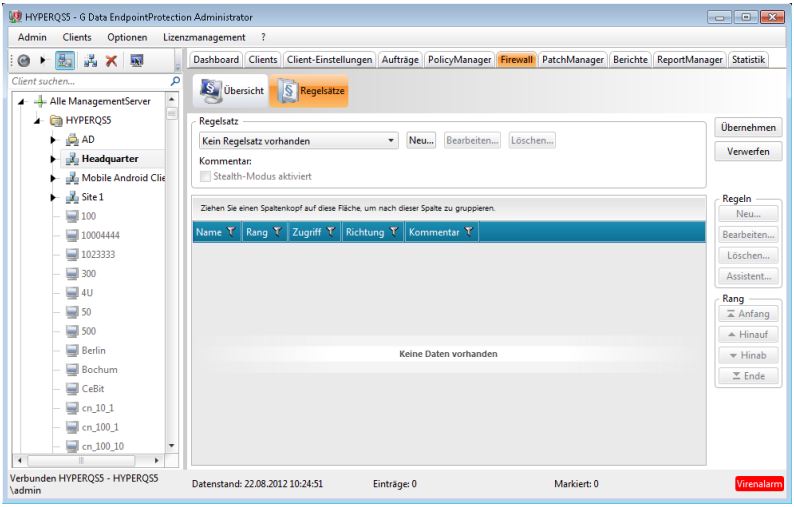
Firewall-Einstellungen

- **Firewall einschalten**: Durch Setzen des Häkchens wird die Firewall auf dem jeweiligen Client aktiviert. Wenn Sie das Häkchen entfernen, ist die Firewall inaktiv.
- **Gesperrte Anwendungen melden**: Wenn dieses Häkchen gesetzt ist und der Client-Rechner mit dem G Data ManagementServer verbunden ist, erhält der Systemadministrator im Bereich **Berichte** Informationen über Anwendungen, die durch die jeweilige Client-Firewall geblockt wurden.
- **Benutzer darf die Firewall ein- und ausschalten**: Hier können Sie als Netzwerkadministrator dem Nutzer des Client-Rechners erlauben, die Firewall zwischenzeitlich auszuschalten. Diese Möglichkeit ist nur dann gegeben, solange sich der Client innerhalb des Firmennetzwerks befindet und sollte natürlich nur versierten Anwendern ermöglicht werden.
- **Offsite-Konfiguration für mobile Clients verwenden**: In der Offsite-Konfiguration werden die Firewall-Regelsätze des Client-Rechners, die in Ihrem Firmennetzwerk gelten, durch Standardregelsätze ersetzt, die automatisch den Umgang mit dem Internet, sicheren-, unsicheren und zu blockierenden Netzen regeln. Auf diese Weise ist der mobile Rechner optimal geschützt, solange er sich nicht im Netzwerk des G Data ManagementServers befindet. Sobald der mobile Rechner wieder mit dem Netzwerk des G Data MangementServers verbunden wird, werden diese Standardregelsätze automatisch wieder durch die Regelsätze ersetzt, wie Sie für diesen jeweiligen Client in Ihrem Netzwerk gelten.

- **Der Anwender darf Offsite-Konfiguration ändern**: Diese Option soll es versierten Anwendern erlauben, ihre Firewall außerhalb des Netzwerks individuell zu konfigurieren. Sobald der mobile Rechner wieder mit dem G Data ManagementServer verbunden wird, werden die durchgeführten Änderungen wieder durch die vom Netzwerkadministrator vorgegebenen Regeln für diesen Client ersetzt. Die Offsite-Konfiguration kann nur verwendet werden, wenn die Firewall im Firmennetz nicht im Autopilot-Modus betrieben wird. Wenn der jeweilige Client im Firmennetzwerk die Autopilot-Einstellungen für die Firewall verwendet, werden die Autopilot-Einstellungen auch dann verwendet, wenn der Client nicht mit dem Netzwerk verbunden ist.

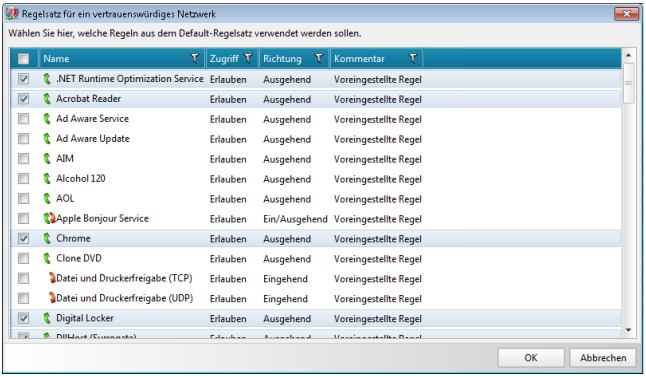
Regelsätze

In diesem Bereich können Sie für verschiedene Netzwerke spezielle Regeln und Regelsätze erstellen.



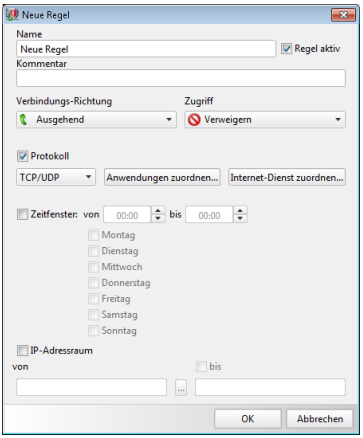
Regelsatz erstellen

Klicken Sie bei **Regelsatz** auf die Schaltfläche **Neu** und Sie haben die Möglichkeit, aus einer großen Anzahl von Default-Regeln und ggf. selbst angelegten Regeln einen individuell auf den Client zugeschnittenen Regelsatz aufzustellen. In der Übersicht wird der jeweilige Regelsatz mit Namen und Stealth-Modus-Status angezeigt. Mit dem **Stealth-Modus** (engl.: verborgen, unbemerkt) werden Anfragen an den Computer, die dazu dienen, die Erreichbarkeit von Ports zu überprüfen, nicht beantwortet. Dies erschwert es Angreifern, auf diese Weise Informationen über das System zu erhalten. Mit Hilfe der Schaltflächen **Neu**, **Löschen** und **Bearbeiten** können Sie bestehende Regelsätze verändern bzw. weitere Regelsätze hinzufügen.


Regelsatz für ein vertrauenswürdiges Netzwerk
Wählen Sie hier, welche Regeln aus dem Default-Regelsatz verwendet werden sollen.
Name
Zugriff
Richtung
Kommentar
.NET Runtime Optimization Service Erlauben Ausgehend Voreingestellte Regel
Acrobat Reader Erlauben Ausgehend Voreingestellte Regel
Ad Aware Service Erlauben Ausgehend Voreingestellte Regel
Ad Aware Update Erlauben Ausgehend Voreingestellte Regel
AIM Erlauben Ausgehend Voreingestellte Regel
Alcohol 120 Erlauben Ausgehend Voreingestellte Regel
AOL Erlauben Ausgehend Voreingestellte Regel
Apple Bonjour Service Erlauben Ein/Ausgehend Voreingestellte Regel
Chrome Erlauben Ausgehend Voreingestellte Regel
Clone DVD Erlauben Ausgehend Voreingestellte Regel
Datei und Druckerfreigabe (TCP) Erlauben Eingehend Voreingestellte Regel
Datei und Druckerfreigabe (UDP) Erlauben Eingehend Voreingestellte Regel
Digital Locker Erlauben Ausgehend Voreingestellte Regel
OK
Abbrechen

Regel erstellen/Regel bearbeiten

Wenn Sie individuelle Regeln erstellen möchten, die Sie dann als Teil eines Regelsatzes auf den Clients verwenden können, klicken Sie bei **Regeln** auf die Schaltfläche **Neu** oder **Bearbeiten**.



Nun erscheint ein Dialog mit folgenden Einstellungsmöglichkeiten:

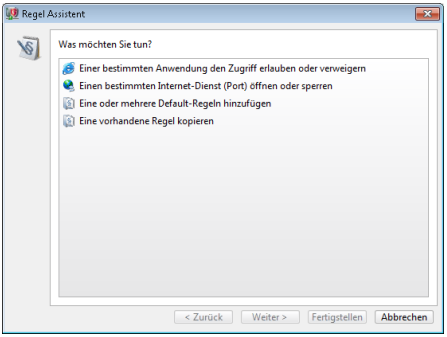
- **Name**: Hier findet sich bei voreingestellten und automatisch generierten Regeln der Programmname für den die jeweilige Regel zutrifft. Sie können den Namen über die **Bearbeiten...**-Schaltfläche auch jederzeit verändern oder um zusätzliche Informationen ergänzen.
- **Regel aktiv**: Sie können eine Regel durch Entfernen des Häkchens inaktiv setzen, ohne sie gleich zu löschen.
- **Kommentar**: Hier erfahren Sie, auf welche Weise die Regel erzeugt wurde. Bei für den Regelsatz voreingestellten Regeln steht **Voreingestellte Regel**, bei Regeln, die sich aus dem Dialog aus dem Firewall-Alarm ergeben steht **per Nachfrage generiert** und für Regeln, die Sie selber über den Profi-Dialog generieren, können Sie einen eigenen Kommentar einfügen.
- **Verbindungs-Richtung**: Mit der **Richtung** wird definiert, ob es sich bei dieser Regel um eine Regel für eingehende, ausgehende oder ein- und ausgehende Verbindungen handelt.
- **Zugriff**: Hier wird eingestellt, ob für das jeweilige Programm innerhalb dieses Regelsatzes der Zugriff erlaubt oder verweigert werden soll.
- **Protokoll**: Hier können Sie auswählen, welchen Verbindungsprotokollen Sie einen Zugriff erlauben oder verwehren wollen. Dabei haben Sie die Möglichkeit, Protokolle generell zu sperren oder freizugeben oder die Verwendung des Protokolls mit der Nutzung einer bestimmten Anwendung oder mehrerer Anwendungen zu verbinden (**Anwendungen zuordnen**). Genauso können Sie die unerwünschten bzw. erwünschten Ports über die Schaltfläche **Internet-Dienst zuordnen** genau definieren.
- **Zeitfenster**: Sie können den Zugriff auf Netzwerkressourcen auch zeitabhängig gestalten und so z.B. dafür sorgen, dass ein Zugriff nur zu Ihren Arbeitszeiten und nicht außerhalb dieser Zeiten erfolgt.
- **IP-Adressraum**: Gerade für Netzwerke mit fest vergebenen IP-Adressen macht es Sinn, deren Nutzung über eine Beschränkung des IP-Adressraumes zu reglementieren. Ein klar definierter IP-Adressraum verringert die Gefahr eines Angriffs deutlich.

Auf diese Weise können Sie individuelle Regeln erstellen, die Sie dann für Ihre Regelsätze auswählen können.

Assistent nutzen

Mit dem Regel Assistenten können Sie auf einfache Weise zusätzliche Regeln für den jeweiligen Regelsatz definieren. Mit dem Regel Assistenten verändern Sie eine oder mehrere Regeln in dem jeweils ausgewählten Regelsatz. Sie erstellen also immer eine Regel innerhalb eines Regelsatzes, der verschiedene Regeln beinhaltet. Abhängig davon, welchen Regelsatz Sie für das jeweilige Netzwerk definiert haben, kann eine

Anwendung in dem einen Regelsatz (z.B. für nicht vertrauenswürdige Netze) gesperrt sein, in dem anderen Regelsatz (z.B. für vertrauenswürdige Netze) vollen Netzzugriff haben. So könnten Sie z.B. einen Browser mit entsprechend unterschiedlichen Regeln so beschränken, dass er wohl auf Seiten zugreifen kann, die in ihrem Heimnetzwerk bereitstehen, aber keine Möglichkeit hat, auf Inhalte aus dem DFÜ-Netzwerk zuzugreifen.


Regel Assistent
Was möchten Sie tun?
Einer bestimmten Anwendung den Zugriff erlauben oder verweigern
Einen bestimmten Internet-Dienst (Port) öffnen oder sperren
Eine oder mehrere Default-Regeln hinzufügen
Eine vorhandene Regel kopieren
< Zurück
Weiter >
Fertigstellen
Abbrechen

Der Regel Assistent stellt folgende Aktionen zur Verfügung:

- **Einer bestimmten Anwendung den Zugriff erlauben oder verweigern**: Hiermit können Sie gezielt eine Anwendung auswählen und ihr im Rahmen des gewählten Regelsatzes den Zugriff auf das Netzwerk erlauben oder verbieten. Wählen Sie im Assistenten dazu einfach das gewünschte Programm aus (Programmpfad) und geben Sie dann unter **Verbindungsrichtung** an, ob das Programm für eingehende Verbindungen, ausgehende Verbindungen oder sowohl ein-, als auch ausgehende Verbindungen gesperrt werden soll. Auf diese Weise können Sie z.B. ihre MP3-Playersoftware ggf. daran hindern, Daten über Ihre Hörgewohnheiten weiterzugeben (ausgehende Verbindungen) oder dafür sorgen, dass nicht automatisch Programmupdates aufgespielt werden (eingehende Verbindungen).
- **Einen bestimmten Internet-Dienst (Port) öffnen oder sperren**: Im Assistenten haben Sie die Möglichkeit, Ports komplett zu sperren oder aber auch nur für eine bestimme Anwendung (z.B. CRM-Software) freizugeben.
- **Eine oder mehrere Default-Regeln hinzufügen**: Bestimmen Sie hier, welche der angelegten Regeln als Default-Regel definiert wird. Default-Regeln werden automatisch vorgeschlagen, wenn ein neuer Regelsatz erstellt werden soll.
- **Eine vorhandene Regel kopieren**: Mit dieser Funktion können Sie zum weiteren Editieren eine Kopie einer bestehenden Regel anfertigen.

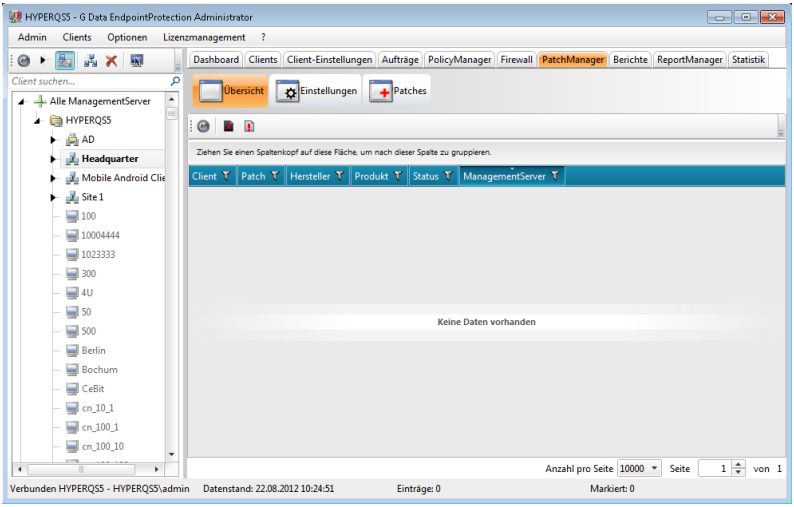
PatchManager

Der PatchManager ist ein optionales Modul für die Nutzer der AntiVirus, ClientSecurity und Endpoint-Protection **Software-Lösungen**.

Mit Hilfe des PatchManagers können Sie die Patch-Implementierung für alle verwalteten Cleints über eine einzige Schnittstelle steuern. Sie können PatchManager sowohl für Updates von Microsoft-Software, als auch anderen Anbietern nutzen. Jeder Patch kann auf Anwendbarkeit überprüft werden, auf eine Blacklist gesetzt werden, distribuiert oder übers Rollback zurückgenommen werden. Dies funktioniert sowohl für einzelne Clients, als auch für Client-Gruppen.

Übersicht

Der Übersichtsbereich bietet Ihnen eine detaillierte Übersicht über Patches und deren Status innerhalb des Netzwerks. Diese umfangreiche Liste kann gefiltert werden, um z.B. zu zeigen ob alle Clients mit allen relevanten Patches aktualisiert wurden. Hier können Sie auch direkt die Patch-Bereitstellung planen.



Der Übersichtsbereich listet alle verfügbaren Patches alphabetisch und einmal pro Client auf. Zum effektiven Verwalten dieser Liste stehen Ihnen verschiedene Filteroptionen zur Verfügung:

Aktualisieren: Hiermit können Sie die Ansicht nach Änderungen aktualisieren und auf den neuesten Stand bringen.

Patches auf der Blacklist ausblenden: Hiermit können Sie in der Übersicht Patches ausblenden, die Sie im Bereich **Patches** auf die Blacklist gesetzt haben.

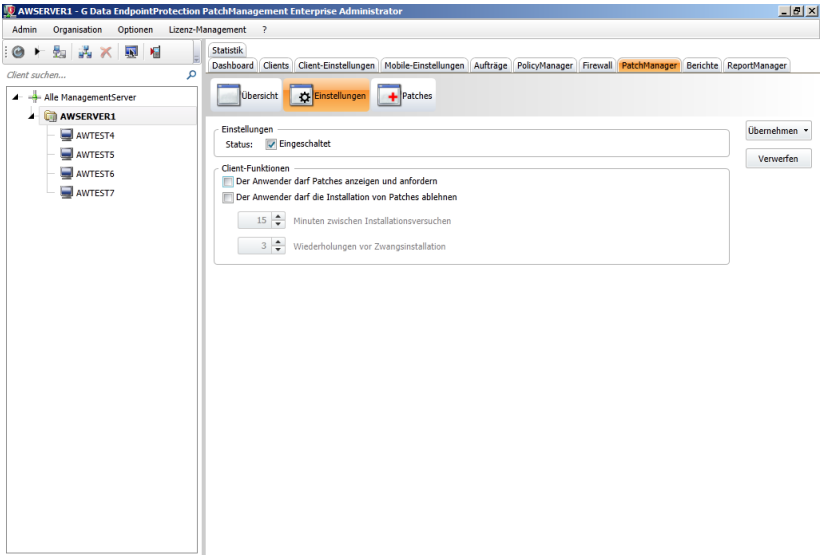
Nur Patches anzeigen: Standardmäßig werden im PatchManager nur Patches und Updates angezeigt. Wenn Sie auch Infos über andere Software-Pakete erhalten möchten, deaktivieren Sie diese Option.

Je nach Patch und Client können verschiedene Arten von Patch-Jobs geplant werden. Führen Sie einen Rechtsklick auf einen oder mehrere Patches aus und wählen Sie dann **Patches auf Usability prüfen** aus, um einen Job auszuführen, der checkt, ob die ausgewählten Patches auf den ausgewählten Clients laufen. Das **Software-Erkennung**-Fenster öffnet sich und Sie können den Job sofort oder zu einem bestimmten Zeitpunkt planen (ggf. mit stündlicher, täglicher, wöchentlicher oder monatlicher Wiederholung). Um einen oder mehrere Patches zu installieren, klicken Sie auf **Patches installieren**. Wie im **Softwareerkennungs**-Fenster können Sie im **Softwareverteilungs**-Fenster die Verteilung von Patches planen. Patches können dabei sofort installiert werden, nach dem nächsten Boot-Vorgang oder nach der nächsten Anmeldung. Optional können Sie Patches auch zeitverzögert installieren. Klicken Sie auf **Rollback** um einen Rollback-Job für Patches zu planen, die bereits verwendet werden. Für weitere Informationen zum jeweiligen Patch klicken Sie bitte auf **Eigenschaften**.

Die Status-Spalte zeigt den Status jedes Patches und seine geplanten oder laufenden Patch-Jobs.

Einstellungen

Hier können Sie bestimmen, wie Patches und Updates auf dem Client und den Gruppen eingespielt werden sollen.



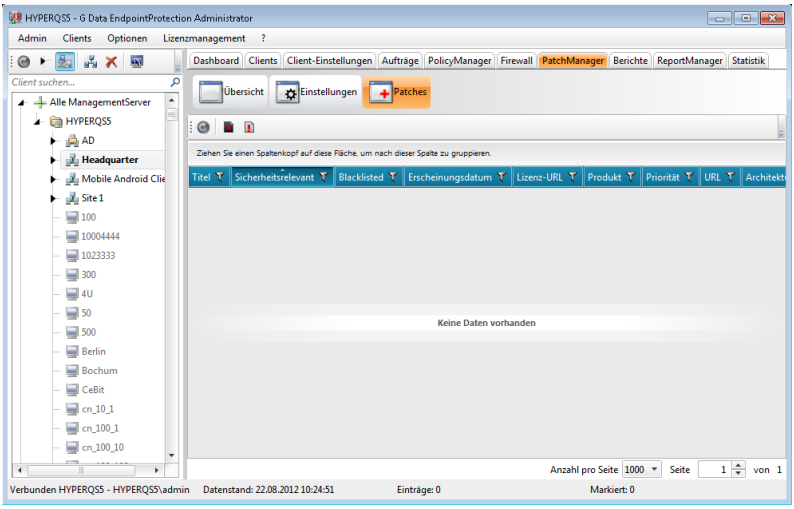
Client-Funktionen

Hier können Sie festlegen, wie viel Ermessensspielraum der Anwender am Client hat.

- **Der Anwender darf Patches anzeigen und anfordern**: Der Anwender kann auf diese Weise aktiv auf benötigte Patches hinweisen.
- **Der Anwender darf die Installation von Patches ablehnen**: Hier können Sie festlegen wie oft und für welchen Zeitraum der Anwender das Installieren von Patches verschieben kann. Prinzipiell ist es dabei nicht möglich, clientseitig das Aufspielen von Patches generell zu unterbinden.

Patches

Im Bereich **Patches** können Sie alle bekannten systemweiten Patches zentral verwalten.



Die Listenansicht ist ähnlich wie die Übersicht aufgebaut. Sie listet alle Patches alphabetisch aus, zeigt aber nicht den Status der Clients. Zum Verwalten der Liste stehen Ihnen mehrere Filter-Optionen zur Verfügung:

Aktualisieren: Hiermit können Sie die Ansicht nach Änderungen aktualisieren und auf den neuesten Stand bringen.

Patches auf der Blacklist ausblenden: Hiermit können Sie in der Übersicht Patches ausblenden, die Sie im Bereich **Patches** auf die Blacklist gesetzt haben.

Nur Patches anzeigen: Standardmäßig werden im PatchManager nur Patches und Updates angezeigt. Wenn Sie auch Infos über andere Software-Pakete erhalten möchten, deaktivieren Sie diese Option.

Führen Sie einen Rechtsklicke auf einen oder mehrere Patches durch und wählen Sie **Patches auf Anwendbarkeit prüfen**, um zu ermitteln, ob die ausgewählten Patches auf den verwalteten Clients verwendet werden können. Das Fenster **Softwareerkennung** öffnet sich dann und ermöglicht Ihnen, den Job sofort oder zu einer bestimmten Zeit (ggf. stündlich, täglich, wöchentlich oder monatlich wiederholt) durchzuführen. Sie können einen oder mehrere Clients auf Patch-Anwendbarkeit geprüft werden.

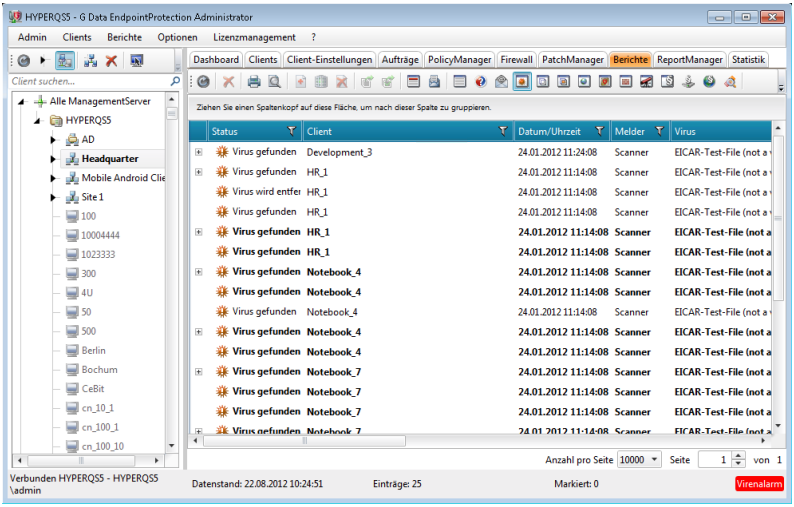
Um einen oder mehrere Patches zu installieren, führen Sie bitte einen Rechtsklick auf die entsprechende Auswahl aus und wählen dann **Patches installieren**. wie bei der Softwareerkennung können Sie auch im Fenster für die **Softwareverteilung** die Distribution von Patches sofort oder zeitlich versetzt (nach dem nächsten Bootvorgang oder dem nächsten Login) duchführen.

Um einen oder mehrere Patches auf eine Blacklist zu setzen, führen Sie einen Rechtsklick auf der Auswahl durch und wählen im nun erscheinenden Kontextmenü **Patches auf die Blacklist setzen**. Um einen Patch von einer Blacklist herunterzunehmen, wählen Sie entsprechend den Eintrag **Patches von der Blacklist entfernen** aus. Um sich weitere Informationen anzeigen zu lassen, wählen Sie im Kontextmenü bitte die Option **Eigenschaften** aus. Hier erhalten Sie Detail-Infos zum Patch inklusive der Lizenz, dem MD5 hash und einer URL für weitere Informationen.

Die Priorität-Spalte zeigt die Priorität jedes Patches. Die hier vorgegebenen Standardprioritäten, die auf den Vorgaben der internen PatchManager-Datenbank basieren, können hier auch von Ihnen geändert werden.

Berichte

Alle Virenfunde, Meldungen des PolicyManagers (wenn eine G Data EndpointProtection installiert ist), sowie alle Firewall-Meldungen (bei G Data ClientSecurity oder EndpointProtection) werden in diesem Aufgabenbereich angezeigt. Darüber hinaus werden zusätzlich systemrelevante Meldungen über Installationen, Berichte, Aufforderungen zum Neustart von Clients usw. hier aufgelistet. In der ersten Spalte der Liste wird der Status des Berichtes angezeigt (z.B. **Virus gefunden** oder **Datei in Quarantäne verschoben**). Sie können auf Virenfunde reagieren, indem Sie die Einträge in der Liste wählen und anschließend im Kontextmenü (rechte Maustaste) oder in der Symbolleiste einen Befehl wählen. So lassen sich beispielsweise infizierte Dateien löschen oder in den **Quarantäne-Ordner** verschieben. Im Aufgabenbereich **Berichte** erscheinen alle Berichte unter den von Ihnen vorgegebenen Namen und lassen sich durch einfaches Klicken auf die jeweilige Spaltenbezeichnung nach unterschiedliche Kriterien sortieren. Die Spalte, nach der die aktuelle Sortierung erfolgt, wird dabei durch ein kleines Pfeilsymbol gekennzeichnet.



In der Menüleiste steht Ihnen für den Aufgabenbereich **Berichte** ein zusätzlicher Menüeintrag zur Verfügung. Für die Funktionen, die mit Dateien operieren (löschen, zurückbewegen etc.) müssen Sie in der Berichtsübersicht die jeweilige Datei bzw. Dateien markieren. Folgende Funktionen können Sie hier auswählen.

- **Ansicht**: Hier können Sie festlegen, ob Sie alle Berichte sehen möchten oder nur eine bestimmte Art von Berichten.
- **Abhängige Berichte ausblenden**: Wenn auf Grund verschiedener Aufträge oder mehrfach durchgeführter Aufträge eine Virenmeldung oder ein Bericht doppelt oder mehrfach angezeigt wird, können Sie hiermit die Duplikate ausblenden. Nur der aktuellste Eintrag wird dann angezeigt und kann bearbeitet werden.
- **Gelesene Berichte ausblenden**: Hier können Sie die Berichte ausblenden, die Sie schon gelesen haben.

Wenn Sie die Scanaufträge auf Ihrem System so eingestellt haben, dass diese den Virenbefall lediglich protokollieren, können Sie die Virenbekämpfung auch manuell durchführen. Wählen Sie dazu im Bericht eine oder mehrere protokollierte Datei/en aus und führen Sie dann die gewünschte Operation durch:

- **Virus aus der Datei entfernen**: Versucht den Virus aus der Originaldatei zu entfernen.

- **Datei in die Quarantäne verschieben**: Diese Funktion verschiebt die ausgewählten Dateien in den Quarantäne-Ordner. Die Dateien werden verschlüsselt im **Quarantäne**-Ordner auf dem G Data ManagementServer gespeichert. Die Originaldateien werden gelöscht. Durch die Verschlüsselung ist sichergestellt, dass der Virus keinen Schaden anrichten kann. Beachten Sie, dass zu jeder Datei in der Quarantäne ein Bericht gehört. Wenn Sie den Bericht löschen wird auch die Datei im Quarantäne-Ordner gelöscht. Sie können eine Datei aus dem Quarantäne-Ordner zur Untersuchung an den **Emergency-AntiViren Service** senden. Öffnen Sie dazu das Kontextmenü eines Quarantäne-Berichts mit einem Rechtsklick. In dem Berichtdialog klicken Sie dann nach Wahl des Einsendegrunds die Schaltfläche **OK**.
- **Datei löschen**: Löscht die Originaldatei auf dem Client.
- **Quarantäne: Säubern und zurückbewegen**: Es wird versucht, den Virus aus der Datei zu entfernen. Wenn dies gelingt, wird die gesäuberte Datei zurück an Ihren Ursprungsort auf dem jeweiligen Client bewegt. Wenn der Virus nicht entfernt werden kann, wird die Datei auch nicht zurückbewegt.
- **Quarantäne: Zurückbewegen**: Verschiebt die Datei aus dem Quarantäne-Ordner zurück auf den Client. **Achtung**: Die Datei wird in ihrem Originalzustand wiederhergestellt und ist weiterhin infiziert.
- **Quarantäne: Zur Internet-Ambulanz senden**: Sollten Sie einen neuen Virus oder ein unbekanntes Phänomen feststellen, senden Sie uns in jedem Fall diese Datei über die Quarantäne-Funktion der G Data Software. Wir analysieren den Virus und werden Ihnen möglichst schnell ein Gegenmittel zur Verfügung stellen. Selbstverständlich behandelt unser **Emergency-AntiViren Service** Ihre eingesandten Daten höchst vertraulich und diskret.
- **Quarantäne: Datei und Bericht löschen**: Löscht die gewählten Berichte. Wenn Berichte gelöscht werden sollen, zu denen eine Quarantäne-Datei gehört, müssen Sie das Löschen noch einmal bestätigen. In diesem Fall werden auch die in Quarantäne befindlichen Dateien gelöscht.
- **Abhängige Berichte löschen**: Wenn auf Grund verschiedener Aufträge oder mehrfach durchgeführter Aufträge eine Virenmeldung oder ein Bericht doppelt oder mehrfach angezeigt wird, können Sie hiermit die doppelten Einträge in der Protokolldatei löschen.

Aktionen und Einstellungen

Folgende Aktionen und Ansichtseinstellungen können Sie in diesem Aufgabenbereich vornehmen:

Aktualisieren: Diese Funktion aktualisiert die Ansicht und lädt die aktuellen **Berichte** vom G Data ManagementServer.

Berichte löschen: Hiermit löschen Sie die ausgewählten Berichte. Wenn Berichte gelöscht werden sollen, zu denen eine Quarantäne-Datei gehört, müssen Sie das Löschen noch einmal bestätigen. In diesem Fall werden auch die in Quarantäne befindlichen Dateien gelöscht.

Drucken: Hiermit starten Sie den Druckvorgang für die Berichte. Sie können in dem erscheinenden Auswahlfenster bestimmen, welche Details und Bereiche Sie ausdrucken lassen möchten.

Seitenansicht: Über die Seitenansicht-Funktion können Sie sich vor dem eigentlichen Ausdruck eine Vorschau der zu druckenden Seiten am Monitor ausgeben lassen.

Virus entfernen

In Quarantäne verschieben

Datei löschen

Datei aus Quarantäne zurückbewegen

Datei säubern und aus Quarantäne zurückbewegen

Abhängige Berichte ausblenden

Gelesene Berichte ausblenden

Alle Berichte anzeigen

Nur Fehler- und Informationsmeldungen anzeigen

Nur Mailberichte anzeigen

Alle Berichte mit nicht entfernten Viren anzeigen

Alle Quarantäne-Berichte anzeigen

Inhalt der Quarantäne anzeigen

Alle HTTP-Berichte anzeigen

Nur BankGuard-Berichte anzeigen

Alle Firewall-Berichte anzeigen (falls Sie eine Softwareversion mit Firewall verwenden)

Nur Berichte der Verhaltensüberwachung anzeigen

Alle Berichte der Anwendungskontrolle anzeigen (falls Sie eine Softwareversion mit Anwendungskontrolle verwenden)

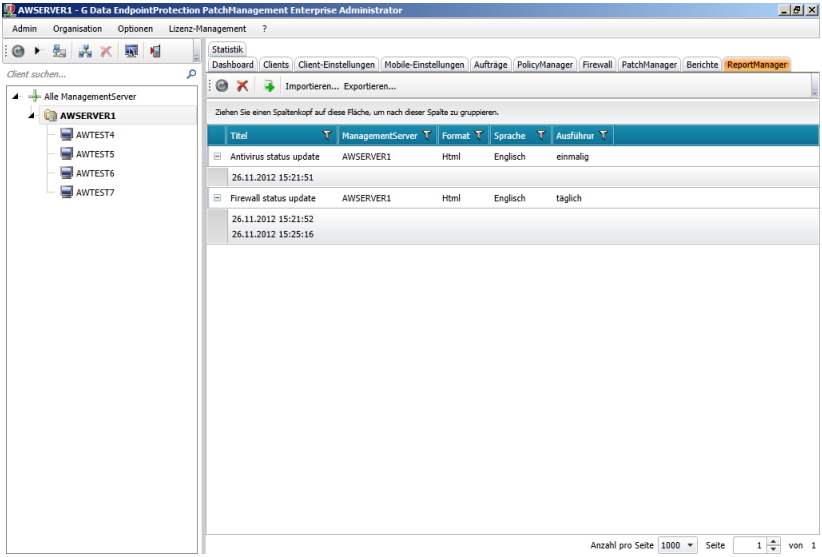
Alle Berichte der Gerätekontrolle anzeigen (falls Sie eine Softwareversion mit Gerätekontrolle verwenden)

Alle Berichte der Web-Inhaltskontrolle anzeigen (falls Sie eine Softwareversion mit Web-Inhaltskontrolle verwenden)

Nur Berichte des Update-/Patch-Managements anzeigen

ReportManager

Über den ReportManager können Sie zeitplangesteuert Berichte über den Status Ihrer Systemsicherheit konfigurieren und an ausgewählte Empfänger verteilen.



Einstellungs- und Ansichtsoptionen

Aktualisieren: Diese Funktion aktualisiert die Ansicht und lädt die aktuelle Reportliste vom G Data ManagementServer.

Löschen: Die Funktion **Löschen...** löscht alle markierten Reports.

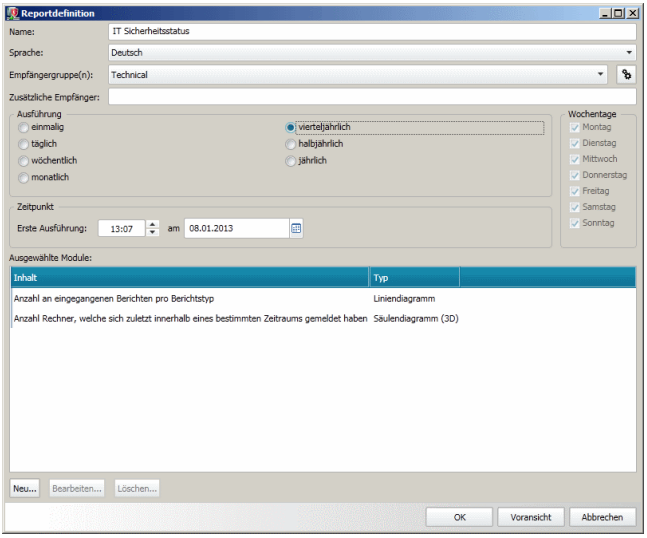
Neue Reportplanung hinzufügen: Hier öffnet sich ein Dialogfenster. Die darin vorhanden Funktionen werden Ihnen im **gleichnamigen Kapitel** erläutert.

Importieren / Exportieren: Hiermit können Sie Einstellungen für den Report importieren und/oder exportieren.

Führen Sie einen Rechtsklick auf einen oder mehrere Berichte durch. Hier können Sie diese löschen oder - mit Auswahl von **Sofort ausführen** - auch direkt noch mal durchführen lassen. Um einen Bericht zu bearbeiten, klicken Sie auf **Eigenschaften**. Über den Eintrag **Verlauf** können Sie auf vorher generierte Berichte zugreifen.

Neue Reportplanung hinzufügen

Hier kann festgelegt werden, welchen Namen der Report haben soll und in welcher Sprache er verfasst werden soll. Unter Empfängergruppen können Sie festlegen, welche Liste von Empfängern diesen Report erhalten soll. Sie können dafür Gruppen verwenden, die Sie unter **Optionen** > **Server-Einstellungen** > **E-Mail-Einstellungen** angelegt haben oder hier auch direkt neue Empfängergruppen definieren, darüber hinaus können Sie über das Eingabefeld **Zusätzliche Empfänger** auch weitere E-Mail-Adressen für den jeweiligen Report hinzufügen (Adressaten werden dabei durch Komma getrennt).



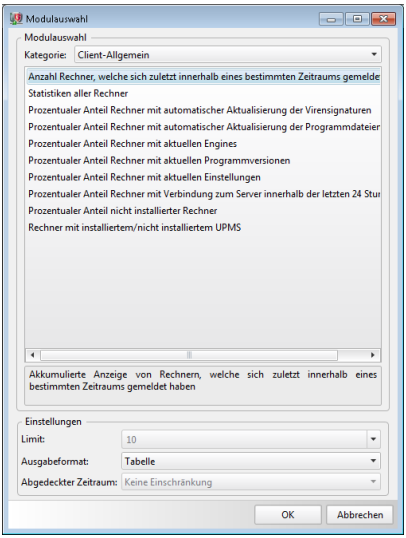
Bei einmaligen Reports können Sie eine Startzeit definieren, bei periodischen Reports können Sie festlegen, wann und in welchem Rhythmus die Benachrichtigung erfolgen soll.

Unter **Täglich** können Sie mit Hilfe der Angaben unter **Wochentage** bestimmen, dass nur an Werktagen einer Report durchführt wird oder eben nur an jedem zweiten Tag oder gezielt an Wochenenden, an denen er nicht zur Arbeit genutzt wird.

Wird ein **einmaliger Report** angelegt, steht nur die Option **Startzeit verwenden** zur Verfügung. Ohne Angabe einer Startzeit wird der Report sofort nach dem Anlegen gestartet.

Modulauswahl

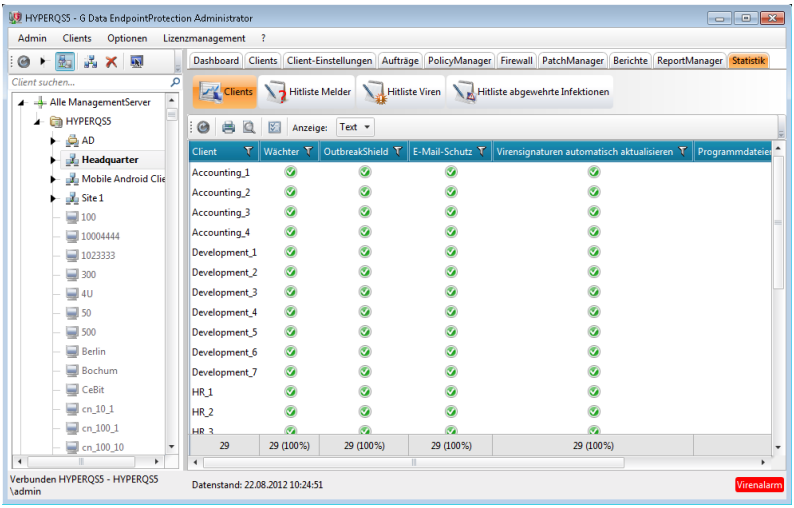
Den Inhalt des jeweiligen Reports definieren Sie, indem Sie unter **Ausgewählte Module** auf die Schaltfläche **Neu** klicken und dort eins der auswählbaren Reportmodule aktivieren. Die Verfügbarkeit der Module ist abhängig von der Produktversion, die Sie verwenden. Die Module für die Reportplanung sind in drei Kategorien untergliedert: **Client-Allgemein**, **Client-Sicherheit** und **PatchManager**. Wählen Sie das entsprechende Modul und konfigurieren Sie die Einstellungen im unteren Bereich des Fensters. Für jedes Modul kann auch ein spezielles Ausgabeformat gewählt werden. Sie haben dabei die Auswahl aus **Tabelle**, **Liniendiagramm (3D)**, **Balkendiagramm (3D)** oder **Kreisdiagramm**. Bitte beachten Sie, dass nicht jedes Modul jedes Ausgabeformat unterstützt. Für manche Module können Sie außerdem ein Limit definieren, um die Menge der dargestellten Daten zu beschränken oder entsprechend einen zeitlichen Rahmen zur Darstellung auswählen. Klicken Sie auf **OK** , um die ausgewählten Module dem jeweiligen Bericht hinzuzufügen. Um Module zu bearbeiten oder zu löschen, stehen Ihnen die entsprechenden Schaltflächen zur Verfügung. Wenn Sie die Auswahl und Einstellung der Module abgeschlossen haben, können Sie sich unter **Vorschau** einen Beispielreport mit den getroffenen Einstellungen durchführen.


Modulauswahl
Modulauswahl
Kategorie:
Client-Allgemein
Anzahl Rechner, welche sich zuletzt innerhalb eines bestimmten Zeitraums gemelde
Statistiken aller Rechner
Prozentualer Anteil Rechner mit automatischer Aktualisierung der Virensignaturen
Prozentualer Anteil Rechner mit automatischer Aktualisierung der Programmdateier
Prozentualer Anteil Rechner mit aktuellen Engines
Prozentualer Anteil Rechner mit aktuellen Programmversionen
Prozentualer Anteil Rechner mit aktuellen Einstellungen
Prozentualer Anteil Rechner mit Verbindung zum Server innerhalb der letzten 24 Stu
Prozentualer Anteil nicht installierter Rechner
Rechner mit installiertem/nicht installiertem UPMS
Akkumulierte Anzeige von Rechnern, welche sich zuletzt innerhalb eines bestimmten Zeitraums gemeldet haben
Einstellungen
Limit:
10
Ausgabeformat:
Tabelle
Abgedeckter Zeitraum:
Keine Einschränkung
OK
Abbrechen

Wenn ein Report-Job durchgeführt wurde, erscheint der erstellte Report in der Übersicht des **ReportManagers** und wird an die ausgewählten Empfänger versendet. Um alle Instanzen eines Reports zu sehen, führen Sie einfach einen Doppelklick auf dem entsprechenden Report aus.

Statistik

In diesem Aufgabenbereich können Sie sich statistische Informationen zum Virenaufkommen und zu Infektionen auf den Clients anzeigen lassen, sowie den Sicherheitsstatus des verwalteten Netzwerks. Es stehen verschiedene Ansichten zur Verfügung: so kann die Darstellung der Informationen in Textform erfolgen oder auch grafisch aufbereitet werden (Säulen- oder Tortendiagramm). Die entsprechende Ansicht lässt sich unter **Anzeige** auswählen. Es stehen Informationen bereit über den Status der **Clients**, über die **Hitliste der Melder**, die **Hitliste der Viren** und über die **Hitliste der abgewehrten Infektionen**. Wählen Sie den entsprechenden Bereich in der Übersicht aus, um die Informationen einzusehen.



G Data WebAdministrator

Der G Data WebAdministrator ist eine webbasierte Steuerungssoftware für den G Data ManagementServer. Mit ihm können Einstellungen für den G Data ManagementServer über ein Webinterface in einem Browser vorgenommen werden.

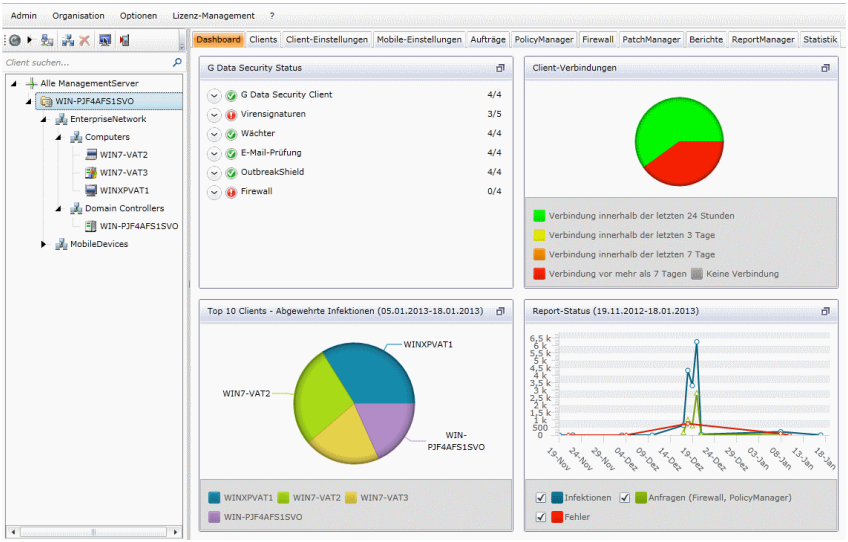
Starten des G Data WebAdministrators

Um den **G Data WebAdministrator** zu nutzen, klicken Sie auf das Desktop-Symbol des G Data WebAdministrators. Alternativ können Sie auch Ihren Internetbrowser starten und die URL ansurfe, die Ihnen beim Abschluss des Installationsprozesses mitgeteilt wurde. Die URL besteht aus der IP-Adresse oder dem Computernamen des Rechners, auf dem ISS ausgeführt wird und der WebAdministrator installiert wurde, sowie dem Ordner-Suffix (z.B. http://10.0.2.150/GDAdmin/). Wenn Sie bis jetzt das Microsoft Silverlight Browser Plugin noch nicht installiert haben, werden Sie nun dazu aufgefordert, es herunterzuladen.

Nun öffnet sich automatisch eine Anmeldeseite für den Zugang zum G Data WebAdministrator. Geben Sie hier nun wie beim regulären G Data Administrator Ihre **Zugangsdaten** ein und klicken Sie dann auf die Schaltfläche **Anmelden**. Der G Data WebAdministrator entspricht in Bedienung und Funktion dem G Data Administrator.

Verwendung des G Data WebAdministrators

Die Programmoberfläche des G Data WebAdministrators ist sehr ähnlich zur Oberfläche des G Data Administrators. Nach dem Einloggen sehen Sie das zentrale Dashboard, welches Ihnen einen Überblick über Ihr Netzwerk, die Clients und den Zustand des G Data ManagementServers bietet.



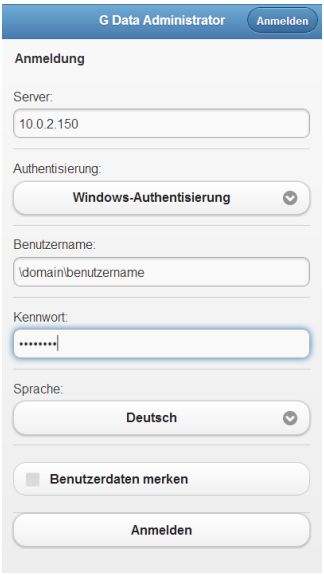
Die Funktionen des WebAdministrators sind identisch zu denen des G Data Administrators. Diese werden im Kapitel **G Data Administrator** umfangreich beschrieben.

G Data MobileAdministrator

Der G Data MobileAdministrator ist die über Smartphones bedienbare Programmoberfläche des G Data ManagementServers. Es kann zum schnellen Bearbeiten und Updaten von Einstelllungen verwendet werden und ist für die Nutzung mit mobilen Geräten optimiert. Dazu sind die wichtigsten und am häufigsten benutzen Funktionen des G Data Administrators so zusammengestellt worden, dass Sie auf einer breiten Palette unterschiedlichster Smartphone-Umgebungen genutzt werden können.

Starten des G Data MobileAdministrators

Nach Abschluss der Installation des G Data MobileAdministrators können Sie diesen von jedem Browser aus aufrufen. Starten Sie dazu Ihren Browser und wählen die URL aus, die Ihnen am Ende des Installationsprozesses mitgeteilt wird. Die URL besteht aus der IP-Adresse oder dem Computernamen des Rechners, auf dem ISS ausgeführt wird und der WebAdministrator installiert wurde, sowie dem Ordner-Suffix (z.B. http://10.0.2.150/GDAdmin/).



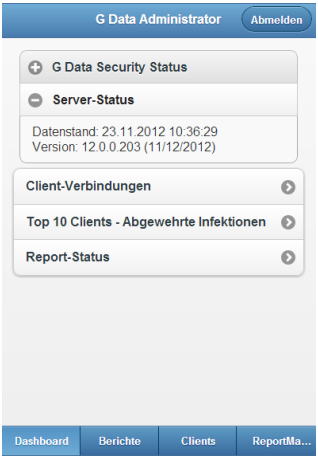
Die Anmeldeseite des MobileAdministrators ist genauso aufgebaut wie die Anmeldeseite des **G Data Administrators** und des **G Data WebAdministrators**. Geben Sie hier bitte den Server, den Benutzernamen, Ihr Kennwort und Ihre Benutzersprache an. Wählen Sie die **Windows-Authentisierung**, wenn Sie sich mit Ihren Domain-Zugangsdaten anmelden möchten, **SQL-Authentisierung**, um sich mit Ihren SQL Server-Anmeldeinformationen anzumelden oder die **Integrierte Authentisierung**, wenn Sie Ihre Zugangsdaten direkt über den Administrator verwalten lassen. Sollten Sie wünschen, dass Ihre Zugangsdaten (bis auf das Kennwort) beim nächsten Öffnen der Anmeldeseite wieder zur Verfügung stehen, wählen Sie bitte **Benutzerdaten merken**.

Verwendung des G Data MobileAdministrators

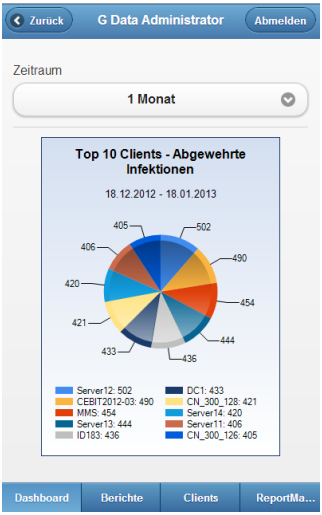
Nach dem Einloggen am G Data MobileAdministrator wird das Hauptmenü angezeigt. Hier stehen Ihnen vier Optionen zur Verfügung: **Dashboard**, **Berichte**, **Clients**, und **ReportManager**. Um das Programm zu beenden, tippen Sie auf die Schaltfläche **Abmelden** oben rechts.

Dashboard

Im Dashboard des G Data MobileAdministrators können Sie die wichtigsten Statistiken über Ihr Netzwerk auf einem Blick einsehen. Vergleichbar der Dashboard-Ansicht im G Data Administrator haben Sie hier einen Überblick über den G Data ManagementServer und dessen Clients. Zusätzlich können Sie sich hier Statistiken über Client-Verbindungen und verhinderte Infektionen anzeigen lassen.



Wählen Sie die Ansicht **G Data Security Status** um eine genauere Übersicht über den Status von Server und Clients zu erhalten. Der MobileAdministrator zeigt Ihnen, wie viele Clients mit dem G Data Security Client ausgestattet sind und bietet Ihnen Informationen über den Aktualisierungsstatus der Virensignaturen und anderer Programmkomponenten (z.B. OutbreakShield, Firewall und Wächter). Sie können über das Öffnen des Virus-Signatur-Unterbereichs auch direkt Engine-Rollbacks durchführen. Der Zustand des ManagementServers an sich kann unter **Server-Status** genauer betrachtet werden.



Weitere Statistiken erhalten Sie unter **Client-Verbindungen** und **Top 10 Clients - Abgewehrte Infektionen**. Tippen Sie auf **Report-Status**, um sich Informationen über Infektionen, Anfragen und Error reports anzeigen zu lassen.

Berichte

In der Berichte-Ansicht finden Sie Reports über Viren, Firewall-Ereignisse und Meldungen des PolicyManagers. Hierbei handelt es sich um eine für mobile Geräte optimierte Darstellung derselben Informationen, die Sie auch im G Data Administrator im **Berichte**-Bereich finden.

Wählen Sie unter **Zeitraum** aus, ob Sie die Reports des letzten Tages, der letzten sieben Tage oder des letzten Monats angezeigt bekommen möchten. Der MobileAdministrator zeigt Ihnen dann an, für welche Kategorie Berichte vorliegen. Wenn Sie eine dieser Kategorien antippen, erhalten Sie eine Übersicht über die aufgezeichneten Ereignisse. Berichte können nach Namen gefiltert werden.

Clients

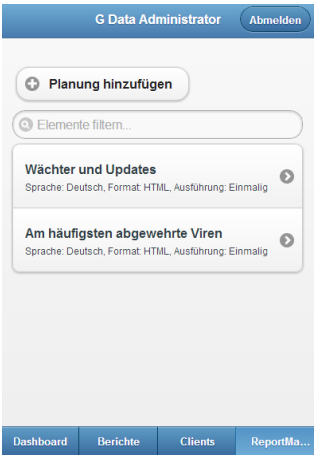
Der MobileAdministrator bietet Ihnen einen genauen Überblick über alle Clients, die vom G Data ManagementServer verwaltet werden. Für jeden Client sind Detailinformationen abrufbar und wichtige Sicherheitseinstellungen können direkt über den MobileAdministrator verändert werden.

In der Übersichtsanzeige können Sie sich eine Liste aller Rechner anzeigen lassen, welche durch den G Data ManagementServer verwaltet werden. Diese Liste kann auch nach Namen gefiltert werden. Wenn Sie einen Client gezielt auswählen, können Sie gezielt für diesen Statistiken über Versionen und Updates einsehen. Darüber hinaus können wichtige Sicherheitseinstellunge direkt verändert werden. So können Sie den **Wächter** ein- oder ausschalten, bestimmen ob **Internetinhalte (HTTP)** verarbeitet werden sollen oder nicht, den **Leerlauf-Scan** aktivieren oder deaktivieren und die **Firewall** ein- oder ausschalten.

Über den Bereich **Anwendungskontrolle** können darüber hinaus **Application control**, **Device control**, **Web content control**, und **Internet usage time** kontrolliert und editiert werden.

ReportManager

Beim ReportManager handelt es sich um die mobile Version des **ReportManager**-Bereichs im G Data Administrator. Hier haben Sie die Möglichkeit, Berichte zu konfigurieren, zu timen und in einer Vorschau zu betrachten.



Um eine neuen Report-Auftrag hinzuzufügen, tippen Sie auf Planung hinzufügen. Schon vorhandene Reports können Sie durch einfaches Antippen zum Editieren auswählen. Dabei stehen Ihnen alle Einstellungsmöglichkeiten zur Verfügung, die auch im ReportManager der Desktopversion möglich sind.

G Data Security Client

Die Client-Software stellt den Virenschutz für die Clients bereit und führt die ihm vom G Data ManagementServer zugewiesenen Jobs ohne eigene Bedienoberfläche im Hintergrund aus. Die Clients verfügen über eigene Virensignaturen und einen eigenen Scheduler, damit auch im Offline-Betrieb (z.B. bei Notebooks, die keine ständige Verbindung zum G Data ManagementServer haben) Virenanalysen durchgeführt werden können.

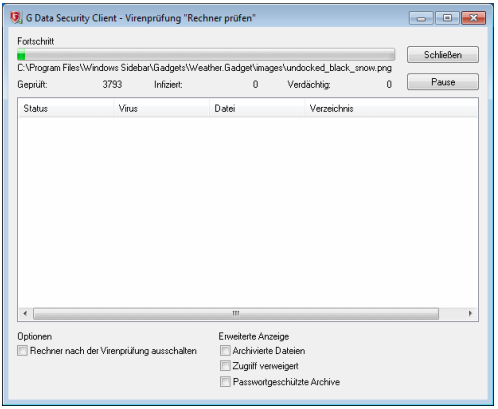
Tray-Icon

Nach der Installation der Client-Software steht dem Benutzer des Clients ein Symbol in der Startleiste zur Verfügung, über welches er unabhängig von den Zeitplänen des Administrators auch selber auf Virenschutz-Funktionen zugreifen kann. Welche Funktionen dem Nutzer zur Verfügung stehen, definieren Sie als Administrator im Bereich **Client-Einstellungen** des G Data Administrators.

Über die rechte Maustaste kann der Benutzer auf diesem G Data Client-Symbol ein Kontextmenü öffnen, das ihm folgende Optionen anbietet.

Virenprüfung

Über diese Option kann der Anwender gezielt mit dem G Data Security Client seinen Rechner auch außerhalb der im G Data Administrator vorgegebenen Prüfzeiträume auf Viren überprüfen.



Der Anwender kann zusätzlich Disketten, CDs/DVDs, den Speicher und Autostart-Bereich, sowie einzelne Dateien oder Verzeichnisse prüfen. Auf diese Weise können auch Notebook-Nutzer, die ihren Rechner nur selten mit dem Firmennetzwerk verbinden, gezielt einen Virenbefall des Systems unterbinden. Über das **Optionen**-Fenster können Client-User so festlegen, welche Aktionen bei einem Virenfund durchgeführt werden sollen (z.B. Verschieben der Datei in den Quarantäne-Bereich.

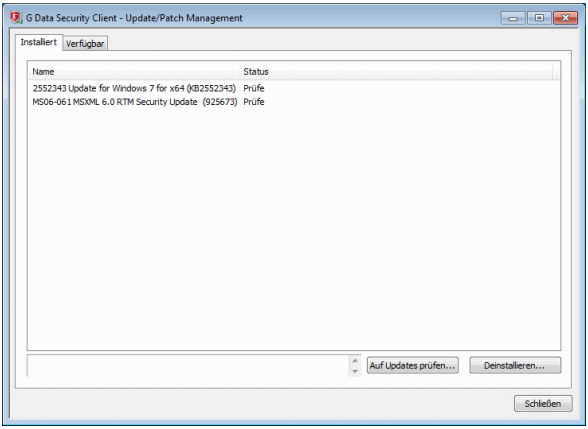
> Der Anwender kann auch aus dem Windows-Explorer heraus Dateien oder Verzeichnisse überprüfen, indem er diese markiert und dann in dem Kontextmenü der rechten Maustaste die Funktion **Auf Viren prüfen (G Data AntiVirus)** verwendet.

Während einer laufenden Virenprüfung wird das Kontextmenü um folgende Einträge erweitert:

- **Priorität Virenprüfung**: Der Anwender hat hier die Möglichkeit, die Priorität der Virenprüfung festzulegen. Bei **Hoch** erfolgt die Virenprüfung schnell, allerdings kann sich das Arbeiten mit anderen Programmen an diesem Rechner deutlich verlangsamen. Bei der Einstellung **Niedrig** dauert die Virenprüfung hingegen vergleichsweise lange, dafür kann währenddessen, ohne größere Einschränkungen, am Client-Rechner weitergearbeitet werden. Diese Option ist nur verfügbar, wenn eine Virenprüfung lokal gestartet wurde.
- **Virenprüfung anhalten**: Diese Option erlaubt es dem Anwender, eine lokal gestartete Virenprüfung eingenständig anzuhalten. Scanaufträge, die vom G Data ManagementServer festgelegt werden, können nur dann angehalten werden, wenn der Administrator beim Anlegen des Jobs die Option **Anwender kann den Job anhalten oder abbrechen** aktiviert hat.
- **Virenprüfung abbrechen**: Diese Option erlaubt es dem Anwender, eine lokal gestartete Virenprüfung eingenständig abzubrechen. Scanaufträge, die vom G Data ManagementServer festgelegt werden, können nur dann abgebrochen werden, wenn der Administrator beim Anlegen des Jobs die Option **Anwender kann den Job anhalten oder abbrechen** aktiviert hat.
- **Scanfenster anzeigen**: Hiermit kann sich der Anwender das Info-Fenster anzeigen lassen, in dem Verlauf und Fortschritt der Virenprüfung angezeigt werden. Diese Option ist nur verfügbar, wenn eine Virenprüfung lokal gestartet wurde.

Updates/Patches

Wenn der Administator sich dazu entscheidet, die Option **Benutzer darf Patches sehen und anfordern** im PatchManager-Modul des G Data Administrators auszuwählen, findet sich im Kontextmenü des Security Client Symbols die Option **Updates/Patches**. Dahinter findet sich eine Übersicht der Updates und Patches für den Client-PC.

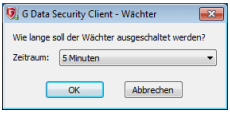


Auf der Registerkarte **Installiert** sehen Sie alle Patches und Updates, welche auf dem System installiert worden sind. Mit einem Doppelklick auf den jeweiligen Eintrag erhalten Sie ausführliche Informationen zum jeweiligen Patch oder Update. Sollte ein Patch oder Update Probleme machen, kann der Anwender es über die Schaltfläche **Deinstallieren** markieren und automatisch dem Administrator zur Deinstallation vorschlagen. Der Status des Patches/Updates wird dann entsprechend aktualisiert und der Administrator erhält einen Report mit einer Rollback-Anfrage. Unabhängig von eventuellen zeit- oder ferngesteuerten Softwareerkennungs-Jobs kann der Anwender über die Schaltfläche **Auf Updates prüfen** auch selber nach aktuellen Patches für sein System suchen.

Auf der Registerkarte **Verfügbar** werden alle Software-Pakete, Patches und Upgrades angezeigt, die für den Client verfügbar sind. Mit einem Doppelklick auf den jeweiligen Eintrag erhalten Sie ausführliche Informationen zum jeweiligen Patch oder Update. Um als Client-Nutzer die Installation aktualisierter Programmdaten zu initiieren, kann dieser hier auf **Installieren** klicken. Der Status des Patches/Updates wird dann entsprechend aktualisiert und der Administrator erhält einen Report mit einer Distributionsanfrage.

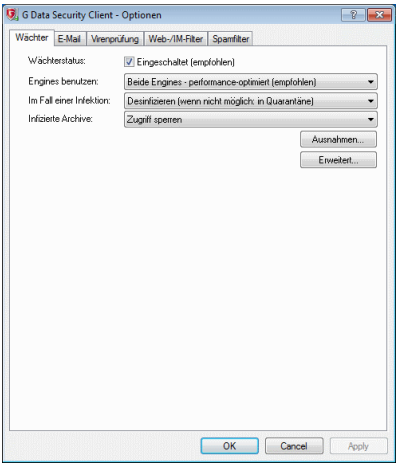
Wächter ausschalten

Über diesen Befehl kann der G Data Wächter vom Anwender für einen gewissen Zeitraum (von **5 Minuten** bis **zum nächsten Neustart des Rechners**) ausgeschaltet werden. Dies ist nur dann möglich, wenn er vom Systemadministrator die entsprechenden Rechte erhalten hat. Das zeitweilige Ausschalten des Wächters kann z.B. bei umfangreichen Dateikopiervorgängen sinnvoll sein, da auf diese Weise der Kopiervorgang beschleunigt wird. Der Echtzeit-Virenschutz ist in diesem Zeitraum allerdings ausgeschaltet.



Optionen

Soweit im G Data Administrator die Option **Der Anwender darf E-Mail und Wächteroptionen ändern** in den **Client-Einstellungen** aktiviert ist, hat der Benutzer des Client-Rechners die Möglichkeit, selber Einstellungen in folgenden Bereichen für seinen Client zu ändern: **Wächter**, **Email**, **Web/IM** und **AntiSpam**. Auf diese Weise können sämtliche Schutzmechanismen der G Data Software auf dem Client ausgeschaltet werden. Diese Option sollte nur fachlich versierten Anwendern zugänglich sein. Die einzelnen Einstellungsmöglichkeiten werden ausführlich im Bereich **Client-Einstellungen** erläutert.



Wenn Sie dem Anwender auf seinem Client die Option **Der Anwender darf selbst Virenprüfungen durchführen** aktivieren, kann dieser unabhängig von den im G Data ManagementServer festgelegten Scanaufträgen seinen Clientrechner auf Viren überprüfen. Die Einstellungen auf dem Karteireiter **Virenprüfung** entsprechen weitestgehend denen, die auch auf dem Karteireiter **Wächter** Verwendung finden.

Die sicherheitsrelevanten Einstellungen unter Optionen... können auch mit einem Passwort geschützt werden. Dazu vergibt der Administrator für den jeweiligen Client ein individuelles Passwort, mit dem der Anwender die Virenkontrollfunktionen auf dem Client verändern kann. Dieses Passwort wird über den Arbeitsbereich Einstellungen im G Data Administrator unter Passwortschutz für die Änderung von Optionen vergeben.

Quarantäne

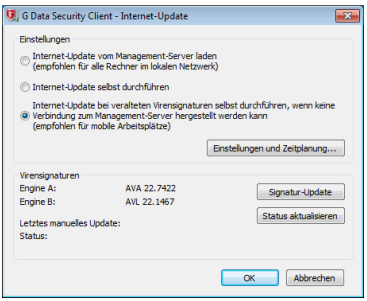
Jeder Client hat einen lokalen Quarantäneordner, in den infizierte Dateien (abhängig von den Einstellungen für Wächter/Scanauftrag) verschoben werden können. Eine Datei, die in Quarantäne verschoben wurde, kann, sofern sie einen Virus enthält, keine Schadroutinen ausführen. Infizierte Dateien werden beim Verschieben in die Quarantäne automatisch gepackt und verschlüsselt. Für die Quarantäne bestimmte Dateien, die größer sind als 1 MB werden automatisch immer in der lokalen Quarantäne des Clients abgelegt, um bei einem massiven Virenbefall das Netzwerk nicht unnötig zu belasten. Alle Dateien, die kleiner als 1 MB sind, werden an den Quarantäneordner des G Data ManagementServers übertragen. Diese Einstellungen sind nicht veränderbar. Die Client-Quarantäne befindet sich im Verzeichnis *%ProgramData%\G DATA\AntiVirusKit Client\Quarantine*. Die G Data ManagementServer-Quarantäne befindet sich im Verzeichnis *%ProgramData%\G DATA\AntiVirus ManagementServer\Quarantine*.

Sollten auf einem mobilen Client ohne Verbindung zum G Data ManagementServer eine infizierte Datei gefunden werden, die kleiner ist als 1 MB, wird sie in der lokalen Quarantäne gespeichert und erst beim nächsten Kontakt zum G Data ManagementServer in die dortige Quarantäne übertragen. Im Quarantäne-Ordner können befallene Dateien desinfiziert werden. Wenn dies nicht funktioniert, lassen sich die Dateien von dort auch löschen und ggf. aus der Quarantäne an ihren Ursprungsort zurückbewegen.

> **Achtung**: Beim Zurückbewegen wird ein Virus nicht entfernt. Sie sollten diese Option nur wählen, wenn das Programm ohne die befallene Datei nicht lauffähig ist und sie diese trotzdem zur Datenrettung benötigen.

Internet-Update

Über den G Data Security Client können auch vom Client-Rechner aus selbstständig Internet-Updates der Virensignaturen durchgeführt werden, falls keine Verbindung zum G Data ManagementServer besteht. Auch diese Option kann vom Netzwerkadministrator für einzelne Clients freigeschaltet werden. Über die Schaltfläche **Einstellungen und Zeitplanung** kann auch die Aktualisierung der Virensignaturen auf dem Client zeitgesteuert ablaufen.


G Data Security Client - Internet-Update
Einstellungen
Internet-Update vom Management-Server laden (empfohlen für alle Rechner im lokalen Netzwerk)
Internet-Update selbst durchführen
Internet-Update bei veralteten Virensignaturen selbst durchführen, wenn keine Verbindung zum Management-Server hergestellt werden kann (empfohlen für mobile Arbeitsplätze)
Einstellungen und Zeitplanung...
Virensignaturen
Engine A: AVA 22.7422
Engine B: AVL 22.1467
Signatur-Update
Status aktualisieren
Letztes manuelles Update:
Status:
OK
Abbrechen

Firewall

Das Firewall-Modul steht Ihnen nur in den **Software-Versionen** ClientSecurity und EndpointProtection zur Verfügung.

Über den Firewallbereich können Anwender umfangreiche Einstellungen in der Firewall ihres Clients vornehmen, wenn diese Option für den jeweiligen Client serverseitig freigeschaltet wurde. Solange sich der Client im Netzwerk des G Data ManagementServers befindet, wird die Firewall zentral vom Server aus administriert. Die Option Firewall steht nur zur Verfügung, wenn im G Data Administrator dem Client die Berechtigung gegeben wurde, die Firewalleinstellungen zu ändern. Für ausführliche Informationen zur Konfiguration und Bedienung der Firewall siehe auch **Firewall-Einstellungen**.

Info

Über Info kann der Versionsstand der installierten G Data Software und der Virensignaturen ermittelt werden.

G Data MailSecurity MailGateway

G Data MailSecurity ist das Softwarepaket zum Komplettschutz Ihrer E-Mail-Kommunikation. Es umfasst:

- G Data MailSecurity MailGateway: Das MailGateway ist der High-End Virenschutz für Ihre Mail-Korrespondenz und verriegelt so den Haupt-Verbreitungsweg moderner Viren effizient und sicher. Es arbeitet als Gateway unabhängig von Ihrem Mail-Server und ist daher mit beliebiger Mail-Server-Software unter Windows, wie auch Linux kombinierbar.
- **G Data MailSecurity Administrator**: Steuerungssoftware für das Mail-Gateway.

G Data MailSecurity MailGateway konfigurieren

Nach Abschluss der Installation steht Ihnen die MailGateway-Software zur Verfügung. Neben der eigentlichen Software, die im Hintergrund läuft, wurde automatisch der **Administrator** installiert, über den Sie vollen Zugriff auf die Funktionen und Optionen des MailGateways haben. Diesen Administrator finden Sie bei einer Standardinstallation unter **Start** > **Programme** > **G Data MailSecurity** > **G Data MailSecurity**. Die Einstellungs- und Einflussmöglichkeiten, die Ihnen über den Administrator zur Verfügung stehen, werden in den folgenden Kapiteln ausführlich erläutert.

Sie können das MailGateway auch über jeden anderen Rechner warten, der die Systemvoraussetzungen für das G Data MailSecurity Administrator-Tool erfüllt. Wenn Sie das MailGateway also über einen anderen Rechner im Netzwerk ansteuern möchten, installieren Sie dort einfach den Administrator ohne die eigentliche MailGateway-Software. Starten Sie dazu einfach erneut das Setup und wählen die Schaltfläche **G Data MailSecurity Administrator** aus. Wenn Sie die Administrator-Software beenden, schließen Sie damit nicht das MailGateway. Dieses bleibt weiterhin im Hintergrund aktiv und steuert die Prozesse, die von Ihnen eingestellt wurden.

Protokolle

Der Empfang und Versand von E-Mails wird in der Regel über die beiden Protokolle SMTP und POP3 abgewickelt. Dabei dient SMTP dazu, Mails an beliebige Empfänger zu verschicken, während POP3 als übergeordnetes Protokoll dazu verwendet wird, eingegangene Mails in einem speziellen Postfach abzulegen, auf welches nur der spezielle Empfänger mittels eines Passwortes Zugriff hat. Je nachdem, wie Ihr Netzwerk aufgebaut ist, kann G Data MailSecurity nun an verschiedenen Knotenpunkten greifen, um eingehende Mails auf Virenbefall zu überprüfen:

- Wenn Sie im Netzwerk einen SMTP-Server verwenden, kann G Data MailSecurity eingehende Mails schon vor dem Erreichen des Mail-Servers überprüfen. Hierzu steht Ihnen die Funktion **Prüfung eingehender Mails (SMTP)** im **Status-Bereich** zur Verfügung.

- Wenn Sie Ihre Mails z.B. über einen aushäusigen Server direkt als POP3-Mails bekommen (z.B. über ein POP3-Sammelkonto), kann G Data MailSecurity auch hier eingreifen, um die POP3-Mails vor dem Öffnen durch den Empfänger auf Virenbefall zu überprüfen. Hierzu steht Ihnen die Funktion **Prüfung eingehender Mails (POP3)** im **Status-Bereich** zur Verfügung.

Selbstverständlich kann G Data MailSecurity auch all Ihre ausgehenden Mails vor dem Versand an die Empfänger auf Virenbefall überprüfen. Da für das Versenden von Mails nur das SMTP-Protokoll Verwendung findet, gibt es hier logischerweise keine POP3-Variante. Hier steht Ihnen die Funktion **Prüfung ausgehender Mails (SMTP)** im **Status-Bereich** zur Verfügung.

Exchange-Unterstützung

Die G Data MailSecurity kann optional auch als Plugin für Microsoft Exchange Server 2007/2010 installiert werden und bietet so proaktiven on-demand und on-access Schutz für alle Mails, die über den Microsoft Exchange Server gesendet und empfangen werden.

G Data MailSecurity Administrator

Der G Data MailSecurity Administrator ist die Steuerungssoftware für das G Data MailSecurity MailGateway, das - vom Systemadministrator zentral gesteuert - den gesamten SMTP- und POP3 basierten E-Mailverkehr mit und in Ihrem gesamten Netzwerk sichert. Der Administrator kann passwortgeschützt von jedem Rechner unter Windows gestartet werden. Als ferngesteuerte Jobs sind alle denkbaren Einstellungsänderungen am Virenscanner und Virensignatur-Updates möglich.

Starten des G Data MailSecurity Administrators

Sie können das AdministratorTool zur Steuerung des MailGateways mit einem Klick auf den Eintrag **G Data MailSecurity Administrator** in der Programmgruppe **Start** > **(Alle) Programme** > **G Data MailSecurity** des Startmenüs aufrufen. Beim Starten des Administrators werden Sie nach dem Server und dem Kennwort gefragt.

Geben Sie in dem Feld **Server**, den Computernamen oder die IP-Adresse des Computers ein, auf dem das MailGateway installiert wurde. Da Sie jetzt noch kein **Kennwort** vergeben haben, klicken ohne Eingabe eines Kennworts einfach auf die **OK**-Schaltfläche. Es öffnet sich ein Kennworteingabefenster, in dem Sie unter **Neues Kennwort** ein neues Kennwort für den G Data MailSecurity Administrator vergeben können. Sie bestätigen das eingegebenen Kennwort durch erneutes Eintippen im Feld **Neues Kennwort bestätigen** und klicken dann auf **OK**. Sie können das Kennwort jederzeit im Bereich **Optionen** in der Karteikarte **Erweitert** mit einem Klick auf die Schaltfläche **Kennwort ändern** neu vergeben.

Weitere Programmstarts

Sie können das AdministratorTool zur Steuerung des MailGateways mit einem Klick auf den Eintrag **G Data MailSecurity Administrator** in der Programmgruppe **Start** > **(Alle) Programme** > **G Data MailSecurity** des Startmenüs aufrufen. Beim Starten des Administrators werden Sie nach dem Server und dem Kennwort gefragt. Geben Sie in dem Feld **Server**, den Computernamen oder die IP-Adresse des Computers ein, auf dem das MailGateway installiert wurde.

G Data MailSecurity Administrator konfigurieren

Die Menüleiste des G Data MailSecurity Administrators bietet Ihnen folgende Optionen:

Optionen: Hier können Sie grundlegende Einstellungen zum Betrieb Ihrer G Data MailSecurity verändern und an individuelle Bedürfnisse anpassen.

Update: Im Internet Update-Bereich können Sie grundlegende Einstellungen zum automatischen Download von aktuellen Virensignaturen aus dem Internet vornehmen. Sie können die Zeitplanungen für diese Downloads individuellen Bedürfnissen anpassen und außerdem Updates der Programmdateien von G Data MailSecurity durchführen.

Spam-Filter: Über den Spam-Filter haben Sie umfangreiche Einstellungsmöglichkeiten, um Mails mit unerwünschten Inhalten oder von unerwünschten Absendern (z.B. Massenmailversendern) wirkungsvoll zu blockieren.

Hilfe: Hier rufen Sie die Online-Hilfe zum Produkt auf.

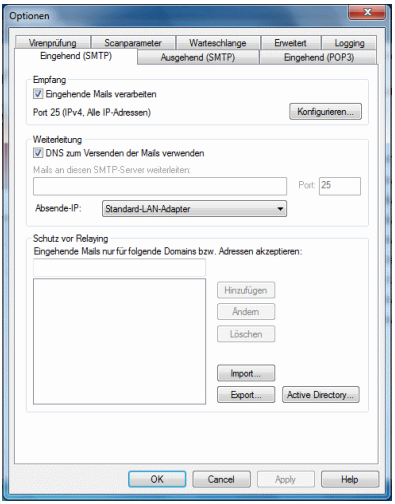
Info: Hier erhalten Sie Informationen zur Programmversion.

Optionen

Im Optionen-Bereich können Sie umfangreiche Einstellungen vornehmen, um G Data MailSecurity optimal auf die Gegebenheiten anzupassen, die in Ihrem Netzwerk existieren. Dazu stehen Ihnen verschiedene thematisch untergliederte Einstellungsbereiche in verschiedenen Karteikarten zur Verfügung, die Sie durch Anklicken des jeweiligen Karteireiters in den Vordergrund holen.

Eingehend (SMTP)

In diesem Bereich haben Sie die Möglichkeit, alle notwendigen Einstellungen zur Virenkontrolle eingehender SMTP-Mails auf Ihrem Mail-Server vorzunehmen.



Empfang

Hier können Sie festlegen, ob eingehende Mails verarbeitet werden sollen. Generell ist hier Port 25 voreingestellt. Sollte auf Grund besonderer Umstände dieser Standardport nicht verwendet werden, können Sie über die Schaltfläche **Konfigurieren** auch andere Port-Einstellungen und Protokoll-Einstellungen für eingehende Mails definieren.

Weiterleitung

Zur Weiterleitung der eingehenden Mails an Ihren Mail-Server deaktivieren Sie bitte die Option **DNS zum Versenden der Mails verwenden** und geben Sie unter **Mails an diesen SMTP-Server weiterleiten** den gewünschten Server an. Geben Sie bitte auch den **Port** an, über den die Mails an den SMTP-Server weitergeleitet werden sollen. Sollten mehrere Netzwerkkarten zur Verfügung stehen, können Sie über die Auswahl unter **Absende-IP** festlegen, welche dieser Karten Sie verwenden möchten.

Schutz vor Relaying

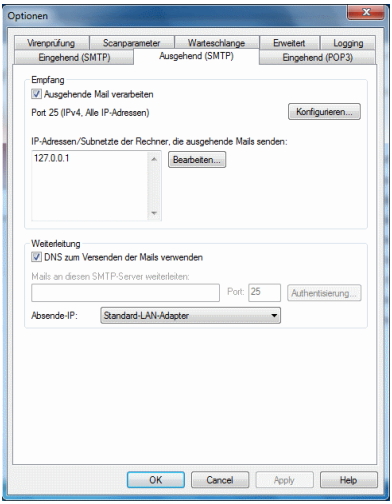
Um einen Missbrauch Ihres Mail-Servers zu unterbinden, können und sollten Sie unter **Eingehende Mails nur für folgende Domains akzeptieren** die Domains festlegen, an die SMTP-Mails versendet werden dürfen. Auf diese Weise kann Ihr Server nicht zur Weiterleitung von SPAM-Mails an andere Domains missbraucht werden.

> **Achtung**: Wenn Sie hier keine Domains eintragen, werden auch keine Mails angenommen. Sollen alle Mails von allen Domains angenommen werden, muss hier ein ***.*** (Sternchen Punkt Sternchen) hinzugefügt werden.

Der Relay-Schutz kann wahlweise auch über eine Liste von gültigen E-Mail-Adressen realisiert werden. Mails für Empfänger, die nicht auf der Liste stehen, werden nicht angenommen. Um die Pflege dieser Mailadressen zu automatisieren, können diese automatisch und periodisch aus dem **ActiveDirectory** gelesen werden. Für die ActiveDirectory-Anbindung wird mindestens das .NET-Framework 1.1 benötigt.

Ausgehend (SMTP)

In diesem Bereich haben Sie die Möglichkeit, alle notwendigen Einstellungen zur Virenkontrolle ausgehender SMTP-Mails auf Ihrem Mail-Server vorzunehmen.



Empfang

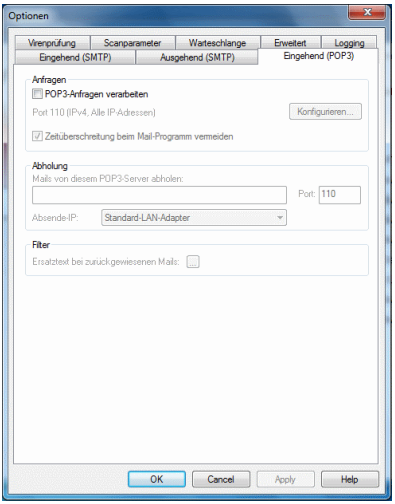
Über das Häkchenfeld **Ausgehende Mail verarbeiten** legen Sie fest, ob Sie ausgehende SMTP-Mails auf Virenbefall kontrollieren möchten oder nicht. Unter **IP-Adressen/Subnetze der Rechner, die ausgehende Mails senden** können Sie bestimmen, von welchen IP-Adressen die zu überprüfenden Mails kommen. Wenn mehrere IP-Adressen dafür in Frage kommen, trennen Sie bitte die einzelnen IP-Adressen durch ein Komma voneinander ab. Diese Eingabe ist nötig, damit das MailGateway eingehende und ausgehende Mails voneinander unterscheiden kann. Generell ist der Port 25 für den Empfang ausgehender Mails voreingestellt. Sollte auf Grund besonderer Umstände dieser Standardport nicht verwendet werden, können Sie über die Schaltfläche **Konfigurieren** auch andere Einstellungen für eingehende Mails definieren.

Weiterleitung

Aktivieren Sie den Eintrag **DNS zum Versenden der Mails verwenden**, damit die Mails direkt an den für die Zieldomäne zuständigen Mail-Server geschickt werden. Wenn Sie die Mails indirekt über ein Relay (z.B. einen Provider) versenden möchten, deaktivieren Sie **DNS zum Versenden der Mails verwenden** und geben Sie unter **Mails an diesen SMTP-Server weiterleiten** das Relay an. Sollten mehrere Netzwerkkarten zur Verfügung stehen, können Sie über die Auswahl unter **Absende-IP** festlegen, welche dieser Karten Sie verwenden möchten.

Eingehend (POP3)

In diesem Bereich haben Sie die Möglichkeit, alle notwendigen Einstellungen zur Virenkontrolle eingehender POP3-Mails auf Ihrem Mail-Server vorzunehmen.



Anfragen

Unter **POP3-Anfragen verarbeiten** aktivieren Sie die Möglichkeit, über G Data MailSecurity Ihre **POP3-Mails** vom entsprechenden POP3-Server abzuholen, auf Viren zu überprüfen und über Ihren Mail-Server an die Empfänger weiterzuleiten. Sie müssen dazu gegebenenfalls den **Port** angeben, den Ihr Mailprogramm für POP3-Anfragen verwendet (in der Regel Port 110). Mit der Funktion **Zeitüberschreitung beim Mail-Programm vermeiden** überbrücken Sie die Zeit, die G Data MailSecurity zum Überprüfen der E-Mails benötigt und verhindern so, dass der Empfänger beim Abruf seiner POP3-Mails möglicherweise vom Mail-Programm einen TimeOut-Fehler enthält, weil die Daten nicht sofort zur Verfügung stehen (sondern je nach Mail-Aufkommen erst ein paar Sekunden verzögert).

POP3-basierte Mailprogramme können manuell konfiguriert werden. Verwenden Sie dabei in Ihrem Mail-Programm 127.0.0.1 bzw. den Server Ihres MailGateways als eingehenden POP3-Server und schreiben Sie den Namen des externen Mail-Servers, mit einem Doppelpunkt getrennt, vor den Benutzernamen. Also z.B. statt *POP3-Server:mail.xxx.de/Benutzername:Erika Musterfrau* schreiben Sie *POP3-Server:127.0.0.1/Benutzername:mail.xxx.de:Erika Musterfrau*. Um eine manuelle Konfiguration durchzuführen, informieren Sie sich bitte auch in der Bedienungsanleitung Ihres Mail-Programms über die notwendigen Schritte für eine manuelle Konfiguration.

Abholung

Unter **Mails von diesem POP3-Server abholen** müssen Sie gegebenenfalls den POP3-Server angeben, von dem Sie die Mails abholen (z.B. *pop3.maildienstanbieter.de*).

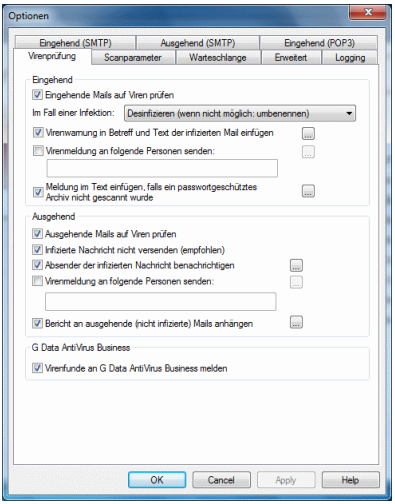
Filter

Wenn POP3-Mails auf Grund einer Content-Prüfung oder auf Grund eines Virenbefalls zurückgewiesen werden, kann der Absender dieser Nachricht automatisch darüber informiert werden. Der Ersatztext bei zurückgewiesenen Mails lautet dabei: *Die Nachricht wurde vom Systemadministrator zurückgewiesen.* Sie können den Text für diese Benachrichtigungsfunktionen aber auch individuell gestalten. Dabei können Sie auch Platzhalter verwenden, die entsprechende Angaben zur zurückgewiesenen Mail in den Benachrichtigungstext übernehmen. Im frei definierbaren Text für den **Betreff** und den **Mailtext** stehen Ihnen folgende Platzhalter (definiert durch ein Prozentzeichen mit einem anschließenden Kleinbuchstaben) zur Verfügung:

- %v > Virus
- %s > Absender
- %r > Empfänger
- %c > Cc
- %d > Datum
- %u > Betreff
- %h > Header
- %i > Absender-IP

Virenprüfung

Bei der Virenprüfung haben Sie die Möglichkeit, Virenprüfungsoptionen für ein- und ausgehende Mails einzustellen.



Eingehend

Grundsätzlich sollten Sie natürlich die Funktion **Eingehende Mails auf Viren prüfen** aktiviert haben und auch darauf achten, welche Option Sie **im Falle einer Infektion** nutzen möchten.

- Nur protokollieren
- Desinfizieren (wenn nicht möglich: nur protokollieren)
- Desinfizieren (wenn nicht möglich: umbenennen)
- Desinfizieren (wenn nicht möglich: löschen)
- Infizierte Anhänge umbenennen
- Infizierte Anhänge löschen
- Nachricht löschen

Optionen, in denen nur ein Protokollieren eingehender Viren stattfindet, sollten Sie nur dann verwenden, wenn Sie Ihr System auf andere Weise permanent vor Virenbefall geschützt haben (z.B. mit dem Client/Server-basierten Virenschutz G Data AntiVirus).

Bei Virenfunden haben Sie eine große Anzahl von Benachrichtigungsoptionen. So können Sie eine Virenwarnung in Betreff und Text der infizierten Mail einfügen, um den Empfänger einer solchen Mail zu informieren. Auch können Sie eine Meldung über den Virenfund an bestimmte Personen senden, also z.B. Systemverwalter oder zuständige Mitarbeiter davon in Kenntnis setzen, dass ein Virus an eine E-Mail-Adresse in ihrem Netzwerk verschickt wurde. Mehrere Empfängeradressen trennen Sie bitte mit einem Semikolon voneinander ab.

Sie können den Text für die Benachrichtigungsfunktionen individuell gestalten. Dabei können Sie auch Platzhalter verwenden, die entsprechende Angaben zur zurückgewiesenen Mail in den Benachrichtigungstext übernehmen. Im frei definierbaren Text für den **Betreff** und den **Mailtext** stehen Ihnen folgende Platzhalter (definiert durch ein Prozentzeichen mit einem anschließenden Kleinbuchstaben) zur Verfügung:

- %v > Virus
- %s > Absender
- %r > Empfänger
- %c > Cc
- %d > Datum
- %u > Betreff
- %h > Header
- %i > Absender-IP

Ausgehend

Grundsätzlich sollten Sie natürlich die Funktion **Ausgehende Mails auf Viren prüfen** aktiviert haben und die Funktion **Infizierte Nachricht nicht versenden** standardmäßig eingeschaltet haben. Auf diese Weise verlässt kein Virus Ihr Netzwerk und richtet möglicherweise bei Geschäftspartnern Schaden. Bei Virenfunden haben Sie eine große Anzahl von Benachrichtigungsoptionen. So können Sie den **Absender der infizierten Mail benachrichtigen** und unter **Virenmeldung an folgende Personen senden** z.B. Systemverwalter oder zuständige Mitarbeiter davon in Kenntnis setzen, dass aus Ihrem Netzwerk ein Virus verschickt werden sollte. Mehrere Empfängeradressen trennen Sie bitte mit einem Semikolon voneinander ab.

Sie können den Text für die Benachrichtigungsfunktionen individuell gestalten. Klicken Sie dazu einfach auf die **...**-Schaltfläche rechts. Dabei können Sie auch Platzhalter verwenden, die entsprechende Angaben zur zurückgewiesenen Mail in den Benachrichtigungstext übernehmen. Im frei definierbaren Text für den **Betreff** und den **Mailtext** stehen Ihnen folgende Platzhalter (definiert durch ein Prozentzeichen mit einem anschließenden Kleinbuchstaben) zur Verfügung:

- %v > Virus
- %s > Absender
- %r > Empfänger
- %c > Cc
- %d > Datum
- %u > Betreff
- %h > Header
- %i > Absender-IP

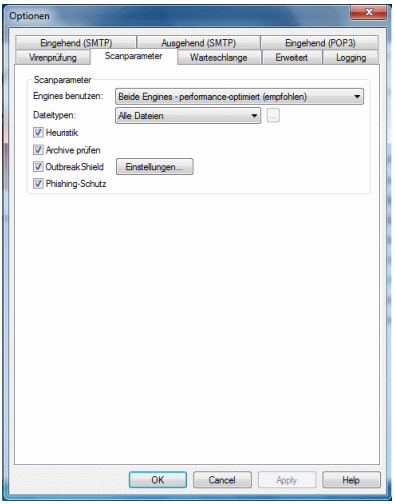
Zusätzlich haben Sie unter **Bericht an ausgehende (nicht infizierte) Mails anhängen** die Möglichkeit, von G Data MailSecurity geprüfte Mails mit einem Bericht am Ende des Mailtextes zu versehen, in dem explizit darauf hingewiesen wird, dass diese Mail von G Data MailSecurity geprüft wurde. Selbstverständlich können Sie diesen Bericht aber auch individuell verändern oder ganz weglassen.

G Data AntiVirus Business

Wenn Sie den Client/Server basierten Virenschutz G Data AntiVirus (z.B. im Rahmen der G Data AntiVirus Business- oder G Data AntiVirus Enterprise-Lösung) installiert haben, können Sie über das Setzen des Häkchens bei **Virenfunde an G Data AntiVirus Business melden** dafür sorgen, dass die Client/Server-basierte Antivirensoftware G Data AntiVirus über Virenfunde des MailGateways benachrichtigt wird und Ihnen auf diese Weise einen umfassenden Überblick über die Virenbelastung bzw. -gefährung Ihres Netzwerkes liefert.

Scanparameter

In diesem Bereich können Sie die Virenerkennungsleistung von G Data MailSecurity optimieren und an persönliche Erfordernisse anpassen. Generell gilt, dass durch eine Verringerung der Virenerkennungsleistung die Performance des Gesamtsystems steigt, während eine Erhöhung der Virenerkennungsleistung möglicherweise leichte Einbußen in der Performance mit sich bringen kann. Hier ist von Fall zu Fall abzuwägen.



Folgende Funktionen stehen Ihnen hier zur Verfügung:

- **Engines benutzen**: G Data MailSecurity arbeitet mit zwei Antiviren-Engines, zwei grundsätzlich unabhängig voneinander operierenden Virenanalyseeinheiten. Unter **Engines benutzen** stellen Sie ein, wie diese miteinander kooperieren. Prinzipiell ist die Verwendung beider Engines der Garant für optimale Ergebnisse bei der Virenprophylaxe. Die Verwendung einer einzigen Engine bringt dagegen Performance-Vorteile mit sich, d.h. wenn Sie nur eine Engine verwenden, kann der Analysevorgang schneller erfolgen.

- **Dateitypen**: Unter **Dateitypen** können Sie festlegen, welche Dateitypen von G Data MailSecurity auf Viren untersucht werden sollen. Wir empfehlen hier die automatische Typ-Erkennung über die automatisch nur die Dateien geprüft werden, die theoretisch auch einen Virus enthalten können. Wenn Sie selber die Dateitypen definieren möchten, für die eine Virenprüfung erfolgen soll, verwenden Sie die Funktion **benutzerdefiniert**. Durch Anklicken der **...**-Schaltfläche können Sie dann eine Dialogbox öffnen, in der Sie die gewünschten Dateitypen ins obere Eingabefeld eintragen und dann über die **Hinzufügen**-Schaltfläche in die Liste der benutzerdefinierten Dateitypen übernehmen. Sie können dabei auch mit **Platzhaltern** arbeiten.

  Das Fragezeichen-Symbol (?) ist Stellvertreter für einzelne Zeichen. Das Sternchen-Symbol (*) ist Stellvertreter für ganze Zeichenfolgen. Um z.B. sämtliche Dateien mit der Dateiendung **exe** prüfen zu lassen, geben Sie also ***.exe** ein. Um z.B. Dateien unterschiedlicher Tabellenkalkulationsformate zu überprüfen (z.B. **xlr**, **xls**), geben Sie einfach ***.xl?** ein. Um z.B. Dateien unterschiedlichen Typs mit einem anfänglich gleichen Dateinamen zu prüfen, geben Sie beispielsweise **text*.*** ein.

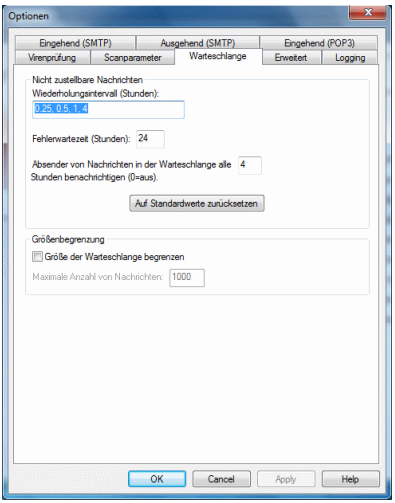
- **Heuristik**: In der Heuristik-Analyse werden Viren nicht nur anhand der ständig aktualisierten Virendatenbanken, sondern auch anhand bestimmter virentypischer Merkmale ermittelt. Diese Methode ist einerseits ein weiteres Sicherheitsplus, andererseits kann sie in seltenen Fällen auch einen Fehlalarm erzeugen.
- **Archive prüfen**: Das Überprüfen **gepackter Dateien** in Archiven sollten generell aktiviert sein.
- **OutbreakShield**: Mit dem OutbreakShield können Schädlinge in Massenmails schon erkannt und bekämpft werden, bevor aktualisierte Signaturen dafür verfügbar sind. Das OutbreakShield erfragt dabei über das Internet besondere Häufungen von verdächtigen Mails und schließt dabei quasi in Echtzeit die Lücke, die zwischen dem Beginn eines Massenmailings und seiner Bekämpfung durch speziell angepasste Signaturen besteht. Wenn Sie **OutbreakShield** verwenden möchten, geben Sie über die Schaltfläche **Einstellungen** an, ob Sie einen Proxyserver verwenden und gegebenenfalls - um OutbreakShield einen jederzeitigen Zugang zum Internet zu ermöglichen - die **Zugangsdaten für die Internetverbindung**. Auf der Registerkarte **OutbreakShield** können Sie den Text der Mail definieren, den ein Mailempfänger enthält, wenn eine an ihn gerichtete Massenmail zurückgewiesen wurde.

Da das OutbreakShield auf Grund seiner eigenständigen Architektur infizierte Mailanhänge nicht desinfizieren, umbenennen oder in die Quarantäne verschieben kann, informiert der Ersatztext den Anwender darüber, dass ihm die verdächtige bzw. infizierte Mail nicht zugestellt wurde. Eine Meldung über vom OutbreakShield zurückgewiesene Mails entfällt, wenn Sie auf der Karteikarte **Virenprüfung** unter **Im Falle einer Infektion** den Punkt **Nachricht löschen** auswählen. In diesem Fall werden alle infizierten Mails, inklusive derer, die ausschließlich vom OutbreakShield erkannt werden, direkt gelöscht.

Warteschlange

In diesem Bereich können Sie festlegen, wie oft und in welchen Abständen der erneute Versand von Mails erfolgen soll, die vom MailGateway nicht an den entsprechenden Mail-Server weitergeleitet werden können.

Generell gelangen Mails erst nach der Virenüberprüfung durch G Data MailSecurity in die Warteschlange. Mails können sich dabei aus verschiedenen Gründen in der Warteschlange befinden. So kann z.B. der Mail-Server, an den Sie nach der Virenprüfung weitergeleitet werden sollen, überlastet oder ausgefallen sein.



Nicht zustellbare Nachrichten

Geben Sie unter **Wiederholungsintervall** an, in welchen Abständen G Data MailSecurity einen neuen Versendeversuch unternehmen soll. So bedeutet z.B. die Angabe *1, 1, 1, 4,* dass G Data MailSecurity die ersten drei Stunden stündlich versucht, die Mail zu verschicken und von da an regelmäßig im Abstand von 4 Stunden. Unter **Fehlerwartezeit** legen Sie fest, wann die Versendung der Mail endgültig abgebrochen und die Mail gelöscht wird.

Sie können **Absender von Nachrichten in der Warteschlangen alle ... Stunden benachrichtigen**, wobei ... ein ganzzahliger Stundenwert sein muss. Wenn Sie die Absender einer nicht zustellbaren Nachricht nicht regelmäßig informieren möchten, geben Sie hier einfach eine *0* ein. Auch wenn Sie die regelmäßige Benachrichtigung von Absendern nicht weitergeleiteter Mails abschalten, wird der Absender natürlich dennoch informiert, wenn seine Mail endgültig nicht zugestellt und vom Server gelöscht wurde.

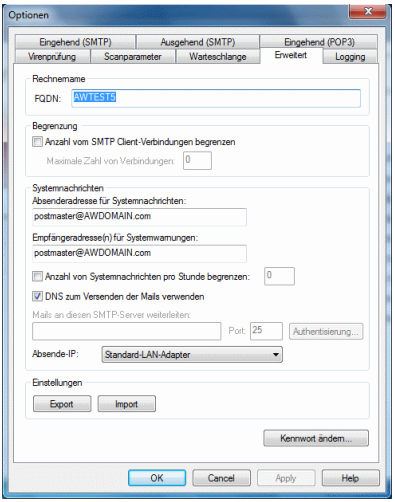
Über die Schaltfläche **Auf Standardwerte zurücksetzen** können Sie die Standardeinstellungen im Bereich Warteschlange wiederherstellen. Diese Einstellungen haben sich in der Praxis bewährt.

Größenbegrenzung

Die Größe der Warteschlange kann auf Wunsch begrenzt werden. Dies dient dem Schutz vor Denial of Service-Attacken. Sollte die Größenbeschränkung überschritten werden, werden keine weiteren Mails mehr in die Warteschlange aufgenommen.

Erweitert

Im Erweitert-Bereich können Sie globale Einstellungen von G Data MailSecurity verändern.



Rechnername

Hier können Sie ggf. den Rechnernamen (FQDN, Full Qualified Domain Name) des Mailservers ändern.

Begrenzung

Um die Anzahl der SMTP-Verbindungen zu begrenzen, die G Data MailSecurity gleichzeitig verarbeitet, setzen Sie bitte das Häkchen vor **Anzahl von SMTP Client-Verbindungen begrenzen**. G Data MailSecurity lässt dann nur die maximale Zahl von Verbindungen zu, die Sie vorgeben. Auf diese Weise können Sie die Mailfilterung an die Leistung der Hardware anpassen, die Sie für das MailGateway verwenden.

Systemnachrichten

Die **Absenderadresse für Systemnachrichten** ist die Mail-Adresse, die z.B. dazu verwendet wird, Absender und Empfänger vireninfizierter Mails zu informieren oder darüber zu informieren, dass sich ihre Mails in der Warteschlange befinden. G Data MailSecurity **Systemwarnungen** sind unabhängig von den allgemeinen Mitteilungen bei Virenfunden. Bei einer Systemwarnung handelt es sich in der Regel um eher globale Informationen, die nicht mit einer einzelnen möglicherweise infizierten Mail in Zusammenhang stehen. So würde G Data MailSecurity z.B. eine Systemwarnung verschicken, wenn die Virenkontrolle aus irgendwelchen Gründen nicht mehr gewährleistet ist. Die Empfängeradresse(n) für Systemwarnungen können durchaus identisch mit den Adressen sein, die Sie unter **Eingehend/Ausgehend (SMTP, POP3)** verwenden.

Einstellungen

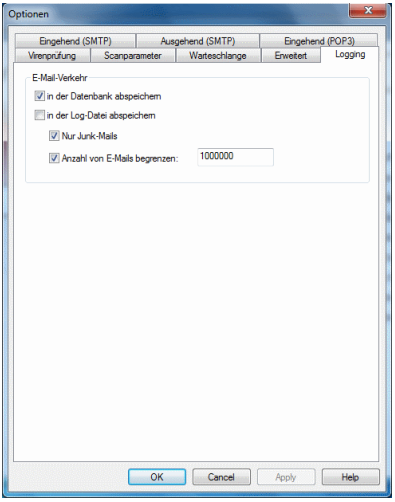
Über die Schaltflächen **Import** und **Export** können Sie die Einstellungen der Programm-Optionen auch als XML-Datei speichern und so ggf. erneut einspielen, wenn der Bedarf gegeben ist.

Kennwort ändern

Hier können Sie das Administrator-Passwort ändern, dass Sie beim ersten Start von G Data MailSecurity vergeben haben. Geben Sie dazu einfach das momentan aktuelle Passwort unter **Altes Kennwort** ein und dann unter **Neues Kennwort** und **Neues Kennwort bestätigen** das neue Kennwort. Mit Anklicken der **OK**-Schaltfläche wird die Kennwortänderung durchgeführt.

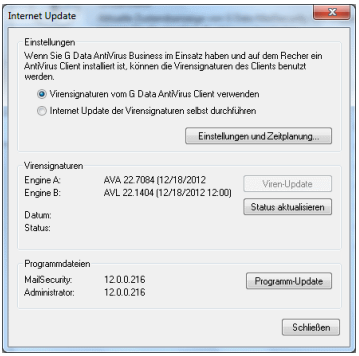
Logging

Im Logging-Bereich können Sie den Mailverkehr auf Ihrem Server statistisch auswerten. Die Ergebnisse dieser Statistikfunktion können Sie im Statistik-Bereich der Programmoberfläche aufrufen, den Sie durch Anklicken der Schaltfläche **Statistik** im Programmbereich **Status** finden. Alternativ können Sie die ermittelten daten auch in einer externen Log-Datei (maillog.txt) abspeichern. Über die Funktionen **Nur Junk-Mails** und **Anzahl von E-Mails begrenzen** können Sie die Größe dieser Log-Datei gegebenenfalls begrenzen.



Update

Im Update-Bereich können Sie umfangreiche Einstellungen vornehmen, um G Data MailSecurity optimal auf die Gegebenheiten anzupassen, die in Ihrem Netzwerk existieren. Hier können Sie die Virensignaturen und Programmdaten von G Data MailSecurity manuell oder automatisiert auf den neuesten Stand bringen.

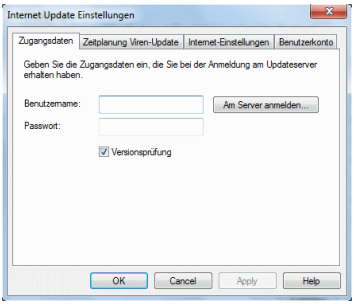


Einstellungen

Hier können Sie grundlegende Einstellungen für das Internet Update vorgeben. Wenn Sie (z.B. im Rahmen der G Data AntiVirus Business-Lösung) parallel zu G Data MailSecurity das Client/Server-basierte G Data AntiVirus verwenden, können Sie sich über **Virensignaturen vom G Data Security Client verwenden** den doppelten Download der Virensignaturen sparen und diese direkt vom installierten G Data Security Client aus erhalten. Über **Internet Update der Virensignaturen selbst durchführen** führt G Data MailSecurity diesen Vorgang selbstständig durch. Über die Schaltfläche **Einstellungen und Zeitplanung** gelangen Sie in einen Bereich, in dem Sie sämtliche notwendigen Einstellungen für manuelle und automatische Internet Updates eingeben können.

Zugangsdaten

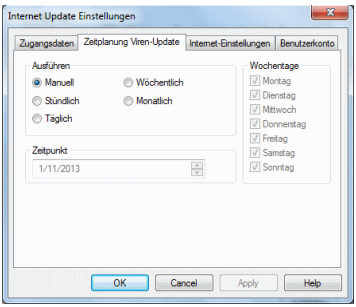
Geben Sie unter Zugangsdaten den **Benutzernamen** und das **Passwort** ein, das Sie bei der Anmeldung von G Data MailSecurity erhalten haben. Mit Hilfe dieser Daten werden Sie vom G Data-Server erkannt und das Update der Virensignaturen kann vollautomatisch erfolgen. Klicken Sie auf die Schaltfläche **Am Server anmelden**, wenn Sie sich noch nicht am G Data-Server angemeldet haben. Geben Sie einfach die Anmeldenummer ein (Sie finden diese auf der Rückseite des Benutzerhandbuches), Ihre Kundendaten und klicken Sie auf **Senden**. Sofort werden Ihnen die Zugangsdaten (Benutzername und Passwort) angezeigt. Sie sollten sich diese Daten aufschreiben und diese sicher verwahren. Für die Anmeldung am Server ist natürlich (wie auch für das Internet Update der Virensignaturen) eine Internetverbindung notwendig.



Zeitplanung Viren-Update

Über die Karteikarte Zeitplanung Viren-Update können Sie festlegen, wann und in welchem Rhythmus das automatische Update erfolgen soll. Unter **Ausführen** geben Sie dazu eine Vorgabe vor, die Sie dann mit den Eingaben unter **Zeitpunkt** spezifizieren.

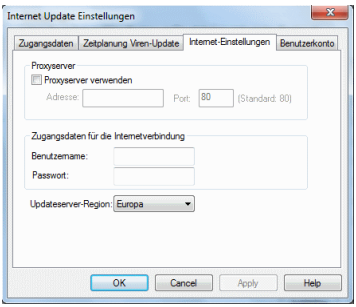
Unter **Täglich** können Sie mit Hilfe der Angaben unter **Wochentage** z.B. bestimmen, dass Ihr Rechner nur an Werktagen das Update durchführt oder eben nur an jedem zweiten Tag oder gezielt an Wochenenden, an denen er nicht zur Arbeit genutzt wird. Um unter **Zeitpunkt** Daten- und Zeiteinträge zu ändern, markieren Sie einfach das Element, das Sie ändern möchten (z.B. Tag, Stunde, Monat, Jahr) mit der Maus und nutzen dann die Pfeiltasten oder die kleinen Pfeilsymbole rechts vom Eingabefeld, um sich im jeweiligen Element chronologisch zu bewegen.



Internet-Einstellungen

Falls Sie einen Rechner hinter einer Firewall verwenden oder andere besondere Einstellungen bezüglich Ihres Internetzugangs haben, verwenden Sie bitte einen **Proxyserver**. Sie sollten diese Einstellung nur ändern, wenn das Internet Update nicht funktioniert. Wenden Sie sich wegen der Proxy-Adresse gegebenenfalls an Ihren Internetzugangsanbieter.

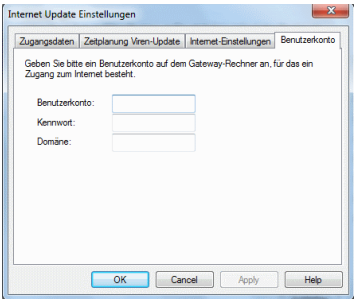
Die Zugangsdaten für die Internetverbindung (Benutzernamen und Passwort) sind gerade beim automatischen Internet Update per Zeitplan sehr wichtig. Ohne diese Angaben kann keine automatische Verbindung mit dem Internet erfolgen. Achten Sie bitte auch darauf, dass Sie in Ihren allgemeinen Interneteinstellungen (z.B. für Ihr Mailprogramm oder Ihren Internetbrowser) die automatische Einwahl ermöglichen. Ohne die automatische Einwahl startet G Data MailSecurity zwar den Internet Update-Vorgang, muss dann aber darauf warten, dass Sie den Aufbau der Internetverbindung mit **OK** bestätigen. Über die Auswahl unter **Updateserver-Region** können Sie einen Updateserver in Ihrer Region auswählen, um ggf. die Datenübermittlung zu optimieren.



Benutzerkonto

Geben Sie bitte unter **Benutzerkonto** ein Benutzerkonto auf dem MailGateway-Rechner an, für das ein Zugang zum Internet besteht.

> **Achtung**: Bitte verwechseln Sie nicht die Angaben, die Sie in den Karteikarten **Zugangsdaten** und **Benutzerkonto** tätigen.



Virensignaturen

Über die Schaltflächen **Viren-Update** und **Status aktualisieren** können Sie auch unabhängig von den Vorgaben, die Sie unter Zeitplanung vorgenommen haben, ein aktuelles Virensignaturupdate starten.

Programmdateien

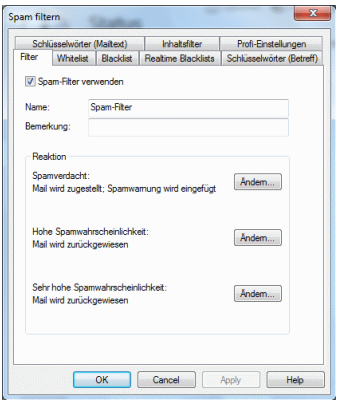
Über die Schaltfläche **Programm-Update** können Sie auch die Programmdateien von G Data MailSecurity aktualisieren, sobald sich hier Änderungen und Verbesserungen ergeben.

Spam-Filter

Über den Spam-Filter haben Sie umfangreiche Einstellungsmöglichkeiten, um Mails mit unerwünschten Inhalten oder von unerwünschten Absendern (z.B. Massenmailversendern) wirkungsvoll zu blockieren. Das Programm prüft viele Merkmale der Mails, die typisch für Spam sind. Anhand der zutreffenden Merkmale wird ein Wert errechnet, der die Wahrscheinlichkeit für Spam widerspiegelt. Dazu stehen Ihnen mehrere Karteikarten zur Verfügung, in denen Ihnen alle relevanten Einstellungsmöglichkeiten thematisch gegliedert zur Verfügung stehen.

Filter

Geben Sie unter **Name** und **Bemerkung** an, wie Sie den Filter nennen möchten und welche zusätzlichen Informationen hierzu vielleicht nötig sind. Unter **Reaktion** können Sie bestimmen, wie der Spam-Filter mit Mails umgehen soll, die möglicherweise Spam enthalten. Dabei können Sie drei Abstufungen vornehmen, die davon beeinflusst werden, wie hoch G Data MailSecurity die Wahrscheinlichkeit dafür ansetzt, dass es sich bei der betreffenden E-Mail um Spam handelt.

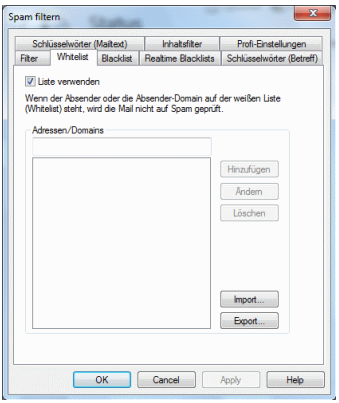


Unter **Spamverdacht** wird der Umgang mit den Mails geregelt, in denen G Data MailSecurity einzelne Spam-Elemente findet. Dabei muss es sich nicht generell um Spam handeln, sondern in seltenen Fällen möglicherweise auch um Newsletter-Mails oder Sammelmailings, die vom Empfänger durchaus erwünscht sind. Hier empfiehlt es sich, den Empfänger auf den Spam-Verdacht hinzuweisen. Unter **Hohe Spamwahrscheinlichkeit** werden die Mails zusammengefasst, die viele Merkmale für Spam in sich vereinen und nur in sehr seltenen Fällen vom Empfänger wirklich erwünscht sind. Unter **Sehr hohe Spamwahrscheinlichkeit** finden sich die Mails, die alle Kriterien einer Spam-Mail erfüllen. Hier handelt es sich so gut wie nie um gewünschte E-Mails und das Zurückweisen von derart gestalteten Mails ist in den meisten Fällen empfehlenswert. Jede dieser drei abgestuften Reaktionen können Sie individuell gestalten.

So haben Sie über **Mail zurückweisen** die Möglichkeit, die Mail gar nicht erst auf Ihren Mail-Server gelangen zu lassen. Der Empfänger erhält diese Mail dann erst gar nicht. Über **Spamwarnung in Betreff und Text der infizierten Mail einfügen** können Sie einen Empfänger einer als Spam identifizierten Mail davon in Kenntnis setzen, dass es sich um Spam handelt. Über die Option **Absender der Nachricht benachrichtigen** können Sie eine automatische Antwortmail an den Absender der als Spam erkannten Mail verschicken, in der Sie diesen darauf hinweisen können, dass seine Mail als Spam erkannt wurde. Da gerade bei Spam viele Mailadressen aber nur einmal verwendet werden, sollten Sie sich überlegen, ob Sie diese Funktion aktivieren. Über die Option **An folgende Personen weiterleiten** können Sie als Spam verdächtige Mails auch automatisch weiterleiten, z.B. an den Systemadministrator.

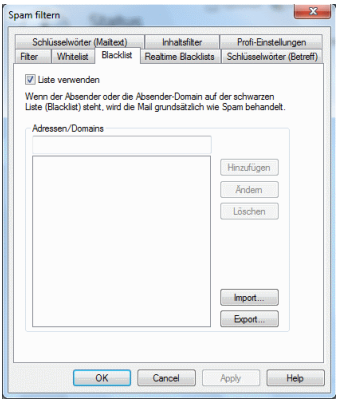
Whitelist

Über die Whitelist können Sie bestimmte Absender-Adressen oder Domains explizit vom Spamverdacht ausnehmen. Geben Sie dazu einfach in das Feld **Adressen/ Domains** die gewünschte E-Mail-Adresse (z.B. *newsletter@gdata.de*) oder Domain (z.B. *gdata.de*) ein, die Sie vom Spamverdacht ausnehmen möchten und G Data MailSecurity behandelt Mails von diesem Absender bzw. dieser Absenderdomain nicht als Spam. Über die **Import**-Schaltfläche können Sie auch vorgefertigte Listen von E-Mail-Adressen oder Domains in die Whitelist einfügen. Die Adressen und Domains müssen in so einer Liste in einzelnen Zeilen untereinander aufgeführt sein. Als Format wird dabei eine einfache txt-Datei verwendet, wie sie z.B. auch mit dem Windows Notepad erstellt werden kann. Über die **Export**-Schaltfläche können Sie eine solche Whitelist auch als Textdatei exportieren.



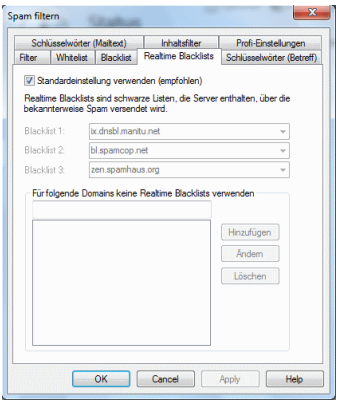
Blacklist

Über die Blacklist können Sie bestimmte Absender-Adressen oder Domains explizit unter Spamverdacht setzen. Geben Sie dazu einfach in das Feld **Adressen/Domains** die gewünschte E-Mail-Adresse (z.B. *newsletter@megaspam.de.vu*) oder Domain (z.B. *megaspam.de.vu*) ein, die Sie unter Spamverdacht setzen möchten und G Data MailSecurity behandelt Mails von diesem Absender bzw. dieser Absenderdomain generell als Mails mit sehr hoher Spamwahrscheinlichkeit. Über die **Import**-Schaltfläche können Sie auch vorgefertigte Listen von E-Mail-Adressen oder Domains in die Blacklist einfügen. Die Adressen und Domains müssen in so einer Liste in einzelnen Zeilen untereinander aufgeführt sein. Als Format wird dabei eine einfache txt-Datei verwendet, wie sie z.B. auch mit dem Windows Notepad erstellt werden kann. Über die **Export**-Schaltfläche können Sie eine solche Blacklist auch als Textdatei exportieren.



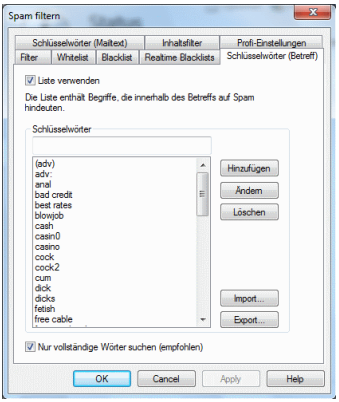
Realtime Blacklists

Im Internet finden sich schwarze Listen, die IP-Adressen von Servern enthalten, über die bekanntermaßen Spam verschickt wird. G Data MailSecurity ermittelt durch DNS-Anfragen an die RBLs (Realtime Blacklists), ob der sendende Server gelistet ist. Falls ja, erhöht sich die Spamwahrscheinlichkeit. Generell sollten Sie hier die Standardeinstellung verwenden, können allerdings auch unter **Blacklist 1**, **2** und **3** eigene Adressen für Blacklists aus dem Internet vergeben.



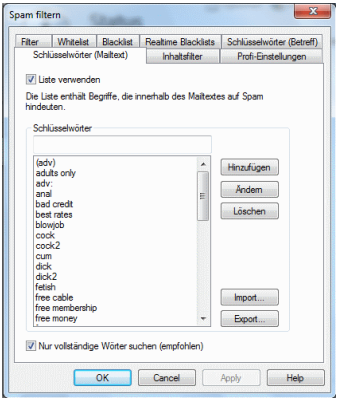
Schüsselwörter (Betreff)

Über die Liste der Schlüsselwörter können Sie Mails auch anhand der in der Betreffzeile verwendeten Wörter unter Spamverdacht stellen. Wenn mindestens einer der Begriffe in der Betreffzeile vorkommt, erhöht sich die Spamwahrscheinlichkeit. Diese Liste können Sie über die Schaltflächen **Hinzufügen**, **Ändern** und **Löschen** beliebig verändern. Über die **Import**-Schaltfläche können Sie auch vorgefertigte Listen von Schlüsselwörtern in Ihre Liste einfügen. Die Einträge müssen in so einer Liste in einzelnen Zeilen untereinander aufgeführt sein. Als Format wird dabei eine einfache txt-Datei verwendet, wie sie z.B. auch mit dem Windows Notepad erstellt werden kann. Über die **Export**-Schaltfläche können Sie eine solche Liste von Schlüsselwörtern auch als Textdatei exportieren. Über das Häkchen vor **Nur vollständige Wörter suchen** können Sie festlegen, dass G Data MailSecurity die Betreffzeile einer Mail nur nach ganzen Wörtern durchsucht, so würde z.B. ein Begriff wie *cash* unter Spamverdacht fallen, während z.B. die gemeinen *Cashew-Kerne* weiterhin unbeanstandet bleiben.



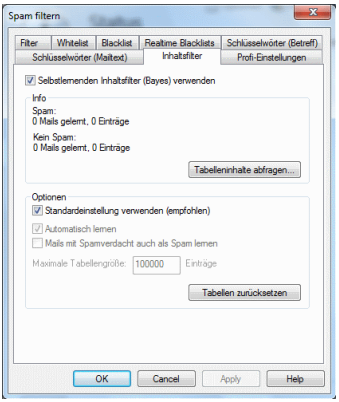
Schlüsselwörter (Mailtext)

Über die Liste der Schlüsselwörter können Sie Mails auch anhand der im ***Mailtext*** verwendeten Wörter unter Spamverdacht stellen. Wenn mindestens einer der Begriffe im Mailtext vorkommt, erhöht sich die Spamwahrscheinlichkeit. Diese Liste können Sie über die Schaltflächen **Hinzufügen**, **Ändern** und **Löschen** beliebig verändern. Über die **Import**-Schaltfläche können Sie auch vorgefertigte Listen von Schlüsselwörtern in Ihre Liste einfügen. Die Einträge müssen in so einer Liste in einzelnen Zeilen untereinander aufgeführt sein. Als Format wird dabei eine einfache txt-Datei verwendet, wie sie z.B. auch mit dem Windows Notepad erstellt werden kann. Über die **Export**-Schaltfläche können Sie eine solche Liste von Schlüsselwörtern auch als Textdatei exportieren. Über das Häkchen vor **Nur vollständige Wörter suchen** können Sie festlegen, dass G Data MailSecurity die Betreffzeile einer Mail nur nach ganzen Wörtern durchsucht, so würde z.B. ein Begriff wie *cash* unter Spamverdacht fallen, während z.B. die gemeinen *Cashew-Kerne* weiterhin unbeanstandet bleiben.



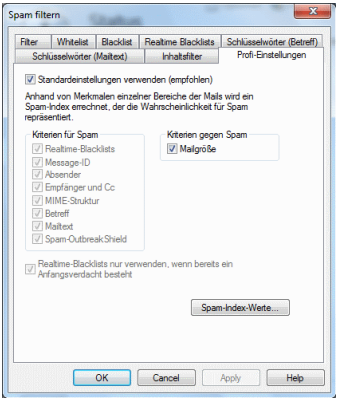
Inhaltsfilter

Beim Inhaltsfilter handelt es sich um einen selbstlernenden Filter auf Basis der Bayes-Methode, der auf Grund der im Mailtext verwendeten Worte eine Spamwahrscheinlichkeit berechnet. Dabei arbeitet dieser Filter nicht allein auf Basis feststehender Wortlisten, sondern lernt bei jeder neu empfangenen Mail weiter dazu. Über die Schaltfläche **Tabelleninhalte abfragen** können Sie sich die Wortlisten anzeigen lassen, die der Inhaltsfilter zur Einordnung einer Mail als Spam verwendet. Über die Schaltfläche **Tabellen zurücksetzen** löschen Sie alle gelernten Tabelleninhalte und der selbstlernende Inhaltsfilter startet den Lernvorgang erneut von Beginn an.



Profi-Einstellungen

In diesem Bereich können Sie die Spamerkennung von G Data MailSecurity sehr detailliert verändern und an die Gegebenheiten Ihres Mail-Servers anpassen. Generell empfiehlt es sich hier jedoch, die Standardeinstellungen zu verwenden. In den Profi-Einstellungen sollten Sie nur dann Veränderungen vornehmen, wenn Sie sich in der Thematik auskennen und genau wissen, was Sie tun.



Programmbereiche

Die Bedienung von G Data MailSecurity ist prinzipiell selbsterläuternd und übersichtlich gestaltet. Anhand unterschiedlicher Karteikarten, die Sie über die links im G Data MailSecurity Administrator angezeigten Symbole anwählen können, wechseln Sie in den jeweiligen Programmbereich und können dort Aktionen durchführen, Voreinstellungen vornehmen oder Vorgänge überprüfen. Folgende Programmbereiche stehen Ihnen zur Verfügung:

- **Status**
- **Filter**
- **Wartenschlangen**
- **Aktivität**
- **Virenfunde**

Status

Im Status-Bereich des Administrators erhalten Sie grundlegende Informationen zum aktuellen Zustand Ihres Systems und des MailGateways. Diese finden sich rechts vom jeweiligen Eintrag als Text-, Zahl- oder Datumsangabe.

Solange Ihre G Data MailSecurity optimal für den Schutz vor Computerviren konfiguriert ist, finden Sie links vor den hier aufgeführten Einträgen ein grünes Ampelsymbol.

Sollte eine Komponente nicht optimal eingestellt sein (z.B. veraltete Virensignaturen, abgeschaltete Virenprüfung), weist Sie ein Achtung-Symbol darauf hin.

Durch doppeltes Anklicken des jeweiligen Eintrags (oder durch Auswählen des Eintrags und Anklicken der **Bearbeiten**-Schaltfläche) können Sie hier direkt Aktionen vornehmen oder in den jeweiligen Programmbereich wechseln. Sobald Sie die Einstellungen einer Komponente mit Achtung-Symbol optimiert haben, wechselt das Symbol im Status-Bereich wieder auf das grüne Ampelsymbol. Folgende Einträge stehen Ihnen zur Verfügung

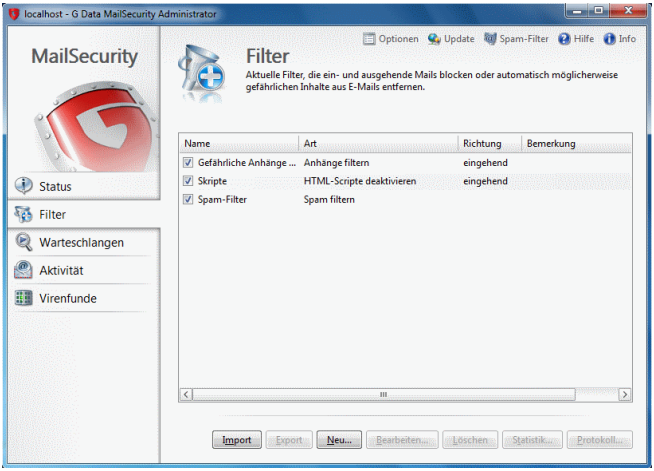
- **Verarbeitung eingehender Mail**: Die Verarbeitung eingehender Mails sorgt dafür, dass Mails vor der Weitergabe an den Empfänger durch das MailGateway überprüft werden. Wenn Sie einen Doppelklick auf diesen Eintrag ausführen, gelangen Sie in das dazugehörige Einstellungsfenster (Menüleiste: **Optionen** > **Eingehend (SMTP)**) und können die Verarbeitung eingehender Mails an individuelle Bedürfnisse anpassen.

- **Virenprüfung eingehender Mail**: Die Prüfung eingehender Mails verhindert, dass infizierte Dateien in Ihr Netz gelangen. Wenn Sie einen Doppelklick auf diesen Eintrag ausführen, gelangen Sie in das dazugehörige Einstellungsfenster (Menüleiste: **Optionen** > **Virenprüfung**) und können die Prüfung eingehender Mails an individuelle Bedürfnisse anpassen.
- **Verarbeitung ausgehender Mail**: Die Verarbeitung ausgehender Mails sorgt dafür, dass Mails vor der Weitergabe an den Empfänger durch das MailGateway überprüft werden. Wenn Sie einen Doppelklick auf diesen Eintrag ausführen, gelangen Sie in das dazugehörige Einstellungsfenster (Menüleiste: **Optionen** > **Ausgehend (SMTP)**) und können die Verarbeitung eingehender Mails an individuelle Bedürfnisse anpassen.
- **Virenprüfung ausgehender Mail**: Die Prüfung ausgehender Mails verhindert, dass aus Ihrem Netz infizierte Dateien verschickt werden. Wenn Sie einen Doppelklick auf diesen Eintrag ausführen, gelangen Sie in das dazugehörige Einstellungsfenster (Menüleiste: **Optionen** > **Virenprüfung**) und können die Prüfung ausgehender Mails an individuelle Bedürfnisse anpassen.
- **OutbreakShield**: Mit dem OutbreakShield können Schädlinge in Massenmails schon erkannt und bekämpft werden, bevor aktualisierte Signaturen dafür verfügbar sind. Das OutbreakShield erfragt dabei über das Internet besondere Häufungen von verdächtigen Mails und schließt dabei quasi in Echtzeit die Lücke, die zwischen dem Beginn eines Massenmailings und seiner Bekämpfung durch speziell angepasste Signaturen besteht.
- **Automatische Updates**: Die Virensignaturen können selbstständig aktualisiert werden. Sie sollten die Option für automatische **Updates** generell aktiviert haben. Wenn Sie einen Doppelklick auf diesen Eintrag ausführen, gelangen Sie in das dazugehörige Einstellungsfenster (Menüleiste: **Internet Update**) und können die Updatefrequenz an individuelle Bedürfnisse anpassen.
- **Datum der Virensignaturen**: Je aktueller die Virensignaturen, desto sicherer ist Ihr Virenschutz. Sie sollten die Virensignaturen so oft wie möglich updaten und diesen Prozess möglichst automatisieren. Wenn Sie einen Doppelklick auf diesen Eintrag ausführen, gelangen Sie in das dazugehörige Einstellungsfenster (Menüleiste: **Internet Update**) und können auch direkt ein Internet Update (unabhängig von etwaigen Zeitplänen) durchführen.
- **Spam-Filter**: Über den **Spam-Filter** haben Sie umfangreiche Einstellungsmöglichkeiten, um Mails mit unerwünschten Inhalten oder von unerwünschten Absendern (z.B. Massenmailversendern) wirkungsvoll zu blockieren.
- **Spam-OutbreakShield**: Mit dem Spam-OutbreakShield können Massenmails schnell und sicher erkannt und bekämpft werden. Das Spam-OutbreakShield erfragt dabei vor dem Abruf von Mails über das Internet besondere Häufungen von verdächtigen Mails ab und lässt diese gar nicht erst in das Postfach des Empfängers gelangen.

Wenn Sie bei der Installation die Option E-Mail-Statistik aktiviert haben, können Sie über die Schaltfläche **Statistik** Zugriff auf die statistische Auswertung Ihres Mailverkehrs bzw. Spamaufkommens nehmen. Das Konfigurieren der Statistk erfolgt dabei im Optionen-Menü des Administrators auf der Registerkarte namens **Logging**.

Filter

Im Filter-Bereich können Sie auf komfortable Weise Filter nutzen, die ein- und ausgehende Mails blocken oder automatisch möglicherweise gefährlichen Inhalte aus Mails entfernen. Die jeweiligen Filter werden in der Liste im Filter-Bereich angezeigt und können über die Häkchenfelder links vom jeweiligen Eintrag beliebig an- bzw. abgeschaltet werden.



- **Import**: Sie können einzelne Filter mit ihren speziellen Einstellungen auch als XML-Datei speichern und ggf. erneut oder auf anderen Rechnern nutzen.
- **Export**: Sie können einzelne Filter mit ihren speziellen Einstellungen auch als XML-Datei speichern und ggf. erneut oder auf anderen Rechnern nutzen. Um mehrere Filter zu exportieren, wählen Sie diese bitte mit der Maus aus und halten dabei die **Strg-Taste** gedrückt.
- **Neu**: Über die **Neu**-Schaltfläche können Sie neue Filterregeln anlegen. Wenn Sie einen neuen Filter anlegen, öffnet sich ein Auswahlfenster, in dem Sie den grundlegenden Filtertyp festlegen können. Alle weiteren Angaben zum zu erstellenden Filter können Sie dann in einem dem Filtertyp angepassten Assistentenfenster angeben. Auf diese Weise erstellen Sie auf sehr komfortable Weise Filter gegen jede erdenkliche Gefährdung.
- **Bearbeiten**: Über die **Bearbeiten**-Schaltfläche können Sie vorhandene Filter bearbeiten.

- **Löschen**: Um einen Filter endgültig zu löschen, markieren Sie diesen bitte mit einem einfachen Mausklick und verwenden dann die **Löschen**-Schaltfläche.
- **Statistik**: Zu jedem Filter können Sie statistische Informationen aufrufen.
- **Protokoll**: Für den **Spam-Filter** gibt es ein Protokoll mit einer Liste, in der die als Spam eingestuften Mails aufgelistet sind. Dem Protokoll kann man auch entnehmen, welche Kriterien für die Einstufung als Spam verantwortlich waren (Spam-Index-Werte). Hier können Sie ggf. bei einer fälschlichen Einstufung einer Mail als Spam den OutbreakShield-Server online darüber informieren, dass hier eine Fehlkennung (False Positive) vorliegt. Die Mail wird dann vom OutbreakShield erneut geprüft und - falls sie tatsächlich fälschlicherweise als Spam erkannt wurde - des Weiteren als unbedenklich eingestuft. Hierbei wird lediglich eine Prüfsumme übermittelt und nicht der Inhalt dieser Mail.

> Selbstverständlich ist Ihr Netzwerk auch unabhängig von individuellen Filterregeln vor Virenbefall geschützt, da G Data MailSecurity ständig im Hintergrund eingehende und ausgehende Mails überprüft. Filterregeln dienen eher dazu, Ihre E-Mail-Accounts vor unerwünschten Mails, Spam und unsicheren Skripten zu bewahren und potentielle Virenherde schon vor der eigentlichen Virenerkennung durch G Data MailSecurity zu minimieren.

Allgemeine Filterfunktionen

Generell können Sie bei allen Filtertypen unter **Name** einen aussagekräftigen Namen für den jeweiligen Filter angeben, mit dem dieser Filter dann in der Liste des Filter-Bereichs angezeigt wird und Sie können unter **Bemerkung** interne Bemerkungen und Notizen zu dem betreffenden Filter angeben. Unter **Richtung** können Sie generell bestimmen, ob eine Filterregel nur für **eingehende Mails**, nur für **ausgehende Mails** oder beide Richtungen gelten soll.

Im Abschnitt **Reaktion** können Sie festlegen, wie mit Mails verfahren werden soll, sobald Sie die Filterkriterien erfüllen, also als Spam-Mails definiert wurden. Sie können dabei den Text für die Funktionen **Absender benachrichtigen** und **Meldung an folgende Personen senden** individuell gestalten. Klicken Sie dazu einfach auf die Schaltfläche rechts von der jeweiligen Reaktion. Dabei können Sie auch Platzhalter verwenden, die entsprechende Angaben zur zurückgewiesenen Mail in den Benachrichtigungstext übernehmen.

Im frei definierbaren Text für den **Betreff** und den **Mailtext** stehen Ihnen folgende Platzhalter (definiert durch ein Prozentzeichen mit einem anschließenden Kleinbuchstaben) zur Verfügung:

%s Absender

%r Empfänger

%c Cc

%d Datum

%u Betreff

%h Header

%i Absender-IP

Die unterschiedlichen Filtertypen werden in den folgenden Abschnitten ausführlich erläutert.

Lesebestätigung filtern

Dieser Filter löscht Lesebestätigungs-Anfragen für eingehende oder ausgehende E-Mails.

HTML-Skripte deaktivieren

Dieser Filter deaktiviert Skripte im HTML-Teil einer Mail. Skripte, die in einer Internetseite durchaus einen Sinn haben mögen, sind - wenn sie in eine HTML-Mail eingebunden sind - eher störend. In manchen Fällen werden HTML-Skripte auch aktiv dazu verwendet, Rechner zu infizieren, wobei Skripte die Möglichkeit haben, sich nicht erst durch das Öffnen einer infizierten Anlage weiterzuverbreiten, sondern alleine schon in der Vorschauansicht einer Mail wirksam werden können.

Externe Referenzen deaktivieren

Viele Newsletter und Produktinformationen im HTML-Mailformat beinhalten Links, die erst dann ausgeführt und angezeigt werden, wenn die Mail geöffnet wird. Dies können z.B. Grafiken sein, die nicht mit der Mail versandt wurden, sondern erst über einen Hyperlink automatisch nachgeladen werden. Da es sich hierbei nicht nur um harmlose Grafiken handeln kann, sondern durchaus auch um Schadroutinen, ist es sinnvoll, diese Referenzen zu deaktivieren. Der eigentliche Mail-Text ist von dieser Deaktivierung nicht betroffen.

Greylist-Filter

Greylist-Filter sind eine effektive Methode, um das Spam-Aufkommen zu reduzieren. Hierbei werden E-Mails von unbekannten Absendern nicht sofort beim ersten Zustellversuch über den SMTP-Server an den Mail-Empfänger übermittelt. Da Spam-Versender in der Regel keine Queue-Verwaltung nutzen und ihre Mails selten ein zweites Mal an denselben SMTP-Server schicken, kann die Anzahl an übermittelten Spam-Mails erheblich sinken.

- **Wartezeiten (Minuten):** Über diese Einstellungen können Sie festlegen, wie lange die Übermittlung verdächtiger Mails blockiert werden soll. Nach Ablauf dieser Zeitspanne wird die Mail bei einem erneuten Sendeversuch dann übermittelt. Wenn der Adressat auf diesen Absender reagiert, wird dieser aus dem Greylist-Filter herausgenommen und in eine Whitelist eingetragen. Nun wird die Zustellung dieser Mails nicht mehr blockiert bzw. verzögert.
- **Lebenszeiten (Tage):** Damit die Whitelist der erwünschten Absender aktuell bleibt, verbleibt eine Absenderadresse nur eine bestimmte Zeit auf der Whitelist, bevor sie wieder auf Greylist-Status gesetzt wird. Der Timer wird für den jeweiligen Absender bei jedem neuen Mailversand wieder zurückgesetzt. Wenn Sie hier z.B. einen Wert über 30 Tage eintragen, können Sie auch erwünschte monatliche Newsletter permanent auf der Whitelist führen.

> Der Greylist-Filter kann nur dann ausgewählt werden, wenn auch der **Spam-Filter** von G Data MailSecurity aktiviert ist. Außerdem muss eine SQL-Datenbank auf dem Server installiert sein.

Anhänge filtern

Beim Filtern von Anhängen haben Sie eine große Auswahl von Möglichkeiten, um Mail-Anhänge (Attachments) und Anlagen zu filtern. Die meisten E-Mailviren verbreiten sich über solche Attachments, die in den meisten Fällen mehr oder minder gut verborgene ausführbare Dateien enthalten. Dabei kann es sich um eine klassische EXE-Datei handeln, die ein Schadprogramm enthält, aber auch um VB-Skripte, die sich unter bestimmten Voraussetzungen sogar hinter vermeintlich sicheren Grafik-, Film- oder Musikdateien verbergen. Generell sollte jeder Anwender bei der Ausführung von Mail-Anhängen große Vorsicht walten lassen und im Zweifelsfall lieber noch einmal eine Rückfrage beim Absender einer Mail durchführen, bevor er eine Datei ausführt, die er nicht ausdrücklich angefordert hat.

Unter **Dateierweiterungen** können Sie die Dateiendungen aufzählen, auf die Sie den jeweiligen Filter anwenden möchten. Dabei können Sie z.B. alle ausführbaren Dateien (z.B. EXE und COM-Dateien) in einem Filter zusammenfassen, aber auch andere Formate (z.B. MPEG, AVI, MP3, JPEG, JPG, GIF etc.) filtern, wenn diese aufgrund Ihrer Größe eine Belastung für den Mail-Server darstellen. Selbstverständlich können Sie auch beliebige Archivdateien (z.B. ZIP, RAR oder CAB) filtern. Trennen Sie bitte alle Dateierweiterungen einer Filtergruppe durch Semikolon, z.B. *.exe; *.dll. Geben Sie unter **Modus** an, ob Sie die unter **Dateierweiterungen** aufgelisteten Dateiendungen erlauben möchten (**Nur angegebene Anhänge erlauben**) oder verbieten (**Angegebene Anhänge filtern**).

Über die Funktion **Auch Anhänge in eingebetteten Mails filtern** sorgen Sie dafür, dass die Filterung der unter **Dateierweiterungen** ausgewählten Anlagentypen auch in Mails stattfindet, die selber eine Anlage einer Mail darstellen. Diese Option sollte generell aktiviert sein. Über **Anhänge nur umbenennen** werden die zu filternden Anlagen nicht automatisch gelöscht, sondern nur umbenannt. Dies ist z.B. bei ausführbaren Dateien (wie z.B. EXE und COM) durchaus sinnvoll, aber auch bei Microsoft Office-Dateien, die möglicherweise ausführbare Skripte und Makros enthalten könnten. Durch das Umbenennen einer Anlage kann Sie nicht unbedacht durch einfachen Mausklick geöffnet werden, sondern muss vom Empfänger erst abgespeichert und ggf. wieder umbenannt werden, bevor er sie verwenden kann. Wenn das Häkchen bei **Anhänge nur umbenennen** nicht gesetzt ist, werden die entsprechenden Anhänge direkt gelöscht.

Unter **Suffix** geben Sie die Zeichenfolge ein, mit der Sie die eigentliche Dateiendung erweitern möchten, auf diese Weise wird die Ausführbarkeit einer Datei durch einfaches Anklicken verhindert (z.B. *.exe_danger). Unter **Meldung im Text der Mail einfügen** können Sie den Empfänger der gefilterten Mail darüber informieren, dass ein Anhang aufgrund einer Filterregel gelöscht oder umbenannt wurde.

Inhaltsfilter

Über den Inhaltsfilter können Sie E-Mails, die bestimmte Themen oder Texte enthalten auf bequeme Weise blocken. Geben Sie dazu unter **Regulärer Ausdruck** einfach die Schlüsselwörter und Ausdrücke ein, auf die G Data MailSecurity reagieren soll und geben Sie unter **Suchbereich** an, in welchen Bereichen einer Mail nach diesen Ausdrücken gesucht werden soll. Über die **Neu**-Schaltfläche rechts vom Eingabefeld für **Regulärer Ausdruck** können Sie auf bequeme Weise Text eingeben, der eine Filteraktion hervorruft. Dabei können Sie Text auf beliebige Weise mit den logischen Operatoren **UND** und **ODER** verknüpfen.

> Wenn Sie z.B. *Alkohol UND Drogen* eingeben, würde der Filter bei einer Mail, die z.B. die Begriffe *Alkohol* und *Drogen* enthält, aktiviert werden, nicht aber bei einer Mail, die nur den Begriff *Alkohol* oder nur den Begriff *Drogen* enthält. Der logische Operator *UND* setzt also voraus, dass alle mit *UND* verknüpften Elemente vorhanden sind, der logische Operator *ODER* setzt lediglich voraus, dass ein Element vorhanden ist.

Sie können auch ohne die Eingabehilfe unter **Regulärer Ausdruck** beliebige Suchbegriffe miteinander kombinieren. Geben Sie dazu einfach die **Suchbegriffe** ein und verknüpfen diese mit den logischen Operatoren. *Oder* entspricht dem Trennstrich | (AltGr + <). *Und* entspricht dem Kaufmanns-Und & (Shift + 6).

Absenderfilter

Über den Absenderfilter können Sie E-Mails, die von bestimmten Absendern kommen, auf bequeme Weise blocken. Geben Sie dazu unter **Adressen/Domains** einfach die E-Mail-Adressen oder Domain-Namen ein, auf die G Data MailSecurity reagieren soll. Mehrere Einträge können Sie durch Semikolon voneinander trennen. Sie können auch Mails ohne Absenderangabe automatisch ausfiltern.

Empfängerfilter

Über den Empfängerfilter können Sie E-Mails für bestimmte Empfänger auf bequeme Weise blocken. Geben Sie dazu unter **Adressen/Domains** einfach die E-Mail-Adressen oder Domain-Namen ein, auf die G Data MailSecurity reagieren soll. Mehrere Einträge können Sie durch Semikolon voneinander trennen. Sie können auch Mails mit leerem Empfängerfeld (also Mails, die nur Bcc- und/oder Cc-Empfänger enthalten) automatisch ausfiltern.

Spam filtern

Über den Spam-Filter haben Sie umfangreiche Einstellungsmöglichkeiten, um Mails mit unerwünschten Inhalten oder von unerwünschten Absendern (z.B. Massenmailversendern) wirkungsvoll zu blockieren. Das Programm prüft viele Merkmale der Mails, die typisch für Spam sind. Anhand der zutreffenden Merkmale wird ein Wert errechnet, der die Wahrscheinlichkeit für Spam widerspiegelt. Dazu stehen Ihnen mehrere Karteikarten zur Verfügung, in denen Ihnen alle relevanten Einstellungsmöglichkeiten thematisch gegliedert zur Verfügung stehen. Die Funktionsweise und Einstellungsmöglichkeiten des Spam-Filters werden im Kapitel **Spam-Filter** ausführlich erläutert.

IP-Filter

Der IP-Filter unterbindet den Empfang von Mails, die von bestimmten Servern abgesendet werden. Der Filter kann sowohl im Blacklist- als auch im Whitelist-Modus verwendet werden. Geben Sie unter **Name** und **Bemerkung** Informationen dazu ein, wieso sie die jeweiligen IP-Adressen sperren möchten und dann jede einzelne IP-Adresse unter **Von folgenden IP-Adressen keine Mails annehmen** ein. Klicken Sie auf **Hinzufügen** und die aktuell eingetragene IP-Adresse wird in die Liste der gesperrten IP-Adressen übernommen. Unter **Modus** können Sie dabei festlegen, ob der IP-Filter im Whitelist-Modus nur bestimmte IP-Adressräume erlauben soll oder im Blacklist-Modus nur bestimmte IP-Adressräume sperren soll. Sie können die Liste der IP-Adressen auch als txt-Datei exportieren oder eine entsprechende txt-Liste mit IP-Adressen importieren.

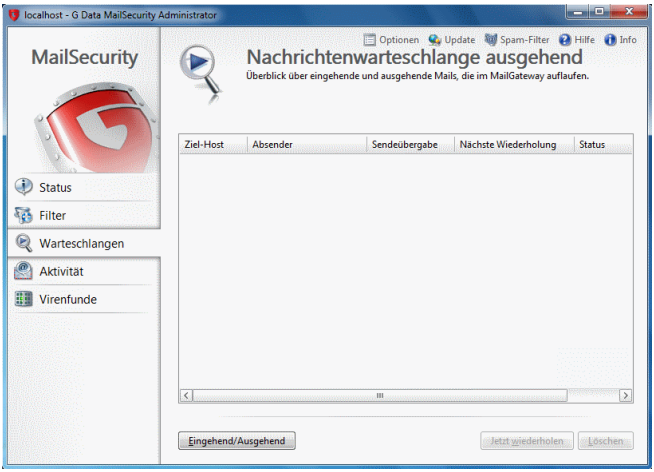
Sprachenfilter

Mit dem Sprachenfilter können Sie automatisch Mails bestimmter Landessprachen als Spam definieren. Wenn Sie also in der Regel z.B. keinen Mailkontakt zu englischsprachigen Personen haben, können Sie über die Definierung von *Englisch* als Spam-Sprache sehr viele Spams ausfiltern. Wählen Sie hier einfach die Sprachen aus, bei denen Sie davon ausgehen, dass Sie in eben diesen Sprachen keine regulären Mails erhalten und G Data MailSecurity erhöht damit die Spameinschätzung für diese Mails erheblich.

Warteschlangen

Im Warteschlangen-Bereich haben Sie jederzeit Überblick über eingehende und ausgehende Mails, die im MailGateway auflaufen und auf Viren und/oder Content überprüft werden. Die Mails werden in der Regel sofort weitergeleitet, durch das MailGateway nur minimal verzögert und dann auch sofort wieder aus der Warteschlangenliste gelöscht. Sobald eine Mail nicht zustellbar ist oder sich Verzögerungen in der Zustellung ergeben (weil der jeweilige Server z.B. momentan nicht erreichbar ist), erfolgt in der Warteschlangenliste ein entsprechender Eintrag. G Data MailSecurity versucht dann in einstellbaren Abständen (unter **Optionen** > **Warteschlange**) die Mail erneut zu verschicken.

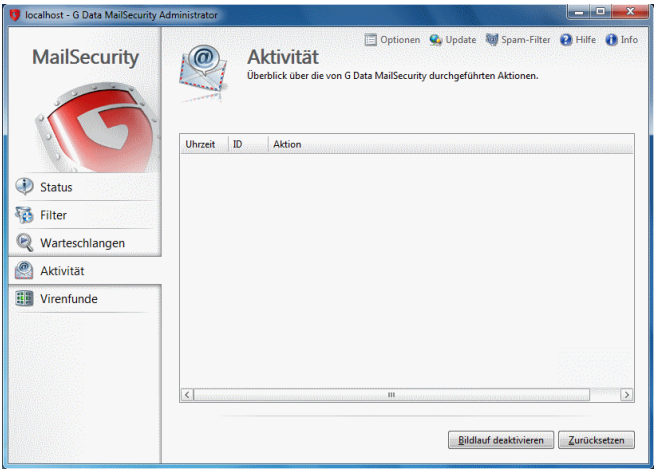
Eine nicht erfolgte oder verzögerte Mailzustellung wird auf diese Weise jederzeit dokumentiert. Über die Schaltfläche **Eingehend/Ausgehend** wechseln Sie von der Listenansicht für eingehende Mails zur Listenansicht für ausgehende Mails. Über die Schaltfläche **Jetzt wiederholen** können Sie eine markierte Mail, die nicht zugestellt werden konnte - unabhängig von den Zeitvorgaben, die Sie für eine erneute Zustellung unter **Optionen** > **Warteschlange** definiert haben - erneut zustellen. Mit der **Löschen**-Schaltfläche entfernen Sie eine nicht zustellbare Mail endgültig aus der Queue.



Aktivität

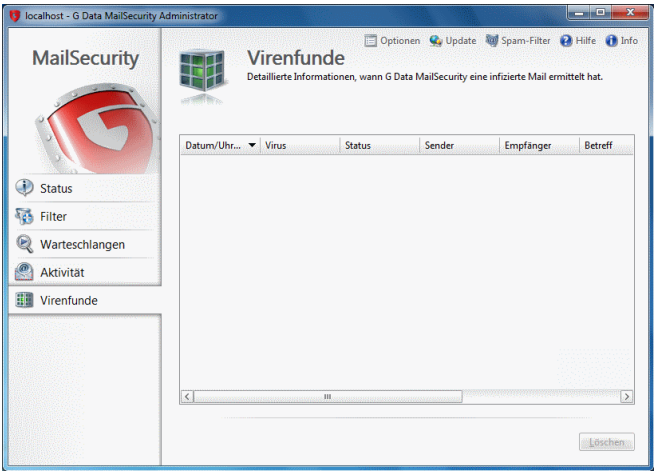
Im Aktivität-Bereich haben Sie jederzeit Überblick über die von G Data MailSecurity durchgeführten Aktionen. Diese werden mit **Uhrzeit**, **ID** und **Aktionsbeschreibung** in der Aktivität-Liste aufgelistet. Mit dem Scrollbalken rechts können Sie in dem Protokoll auf und abscrollen. Über die **Zurücksetzen**-Schaltfläche löschen Sie das bis dahin erzeugte Protokoll und G Data MailSecurity beginnt die Aufzeichnung der Aktivitäten erneut. Mit der Funktion **Bildlauf deaktivieren** wird die Liste weiterhin aktualisiert, aber die neuesten Aktivitäten werden nicht direkt an erster Stelle eingeblendet. Sie können dann konzentrierter in der Liste scrollen.

Über die **ID** können Sie die protokollierten Aktionen eindeutig einzelnen Mails zuordnen. So gehören Vorgänge mit gleicher ID immer zusammen (z.B. 12345 Lade Mail, 12345 Verarbeite Mail, 12345 Sende Mail).



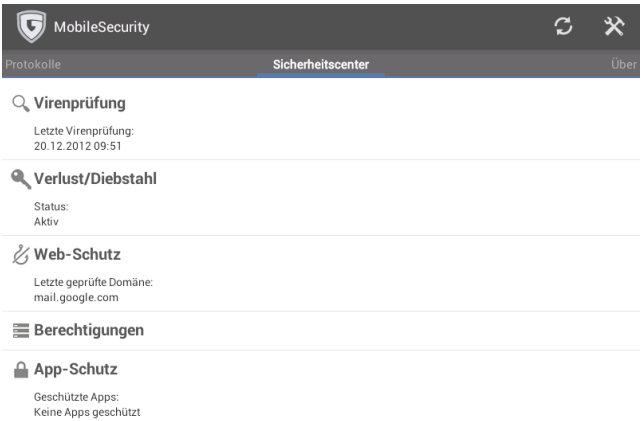
Virenfunde

Im Virenfunde-Bereich werden sie detailliert darüber informiert, wann G Data MailSecurity eine infizierte Mail ermittelt hat, welche Maßnahmen dahingehend erfolgten, um welche Art von Virus es sich handelt und wer die eigentlichen Sender und Empfänger dieser betreffenden Mail sind. Über **Löschen** entfernen Sie die jeweils ausgewählte Virenmeldung aus der Virenfunde-Liste.



G Data MobileSecurity

Mit dieser App erhalten Sie eine speziell auf die G Data Netzwerklösung zugeschnittene Version der **G Data MobileSecurity for Android** App und können so Netzwerksicherheit auch über das G Data's Mobile Device Management realisieren. Die Installation der App erfolgt über den **G Data Administrator**.



Über das Sicherheitscenter der G Data MobileSecurity haben Sie Zugriff auf alle Funktionen der Software. Durch Streichen nach links kann das **Protokolle**-Modul geöffnet werden. Streichen nach rechts öffnet die Versions-Info. Über die Schaltfläche am oberen rechten Rand des Bildschirms können Sie nach aktuellen Updates für die App suchen und das **Einstellungen-Menü** aufrufen.

G Data MobileSecurity konfigurieren

Einstellungen

Die meisten Einstellungen der G Data MobileSecurity können direkt über den **Mobile-Einstellungen** Bereich des G Data Administrators durchgeführt werden. Auf dem Mobilgerät haben Sie darüber hinaus auch die Möglichkeit, einige Einstellungen vorzunehmen.

Allgemein

Benachrichtigungssymbol: Zeigt das Logo der G Data MobileSecurity in der Benachrichtigungsleiste an.

Protokolle speichern: Speichert die durch die Systemüberprüfung erstellten Protokolle.

Automatisches Update

Automatisches Update (auch über die **Mobile-Einstellungen** des Administrators): Virus-Signaturen werden automatisch im Hintergrund aktualisiert.

Update-Häufigkeit (auch über die **Mobile-Einstellungen** des Administrators): Die Update-Frequenz für Updates wird hier eingestellt (**1**, **3**, **7**, **14**, oder **30** Tage).

Nur über WLAN (auch über die **Mobile-Einstellungen** des Administrators): Updates werden nur dann durchgeführt, wenn eine WLAN-Verbindung besteht.

Server-Region: Wählen Sie hier den am nächsten liegenden Update-Server aus (nicht aktiv, wenn die Remote-Administration aktiviert wurde).

Virenprüfung

Periodische Virenprüfung (auch über die **Mobile-Einstellungen** des Administrators): Öffnet das Einstellungsmenü des Moduls **Virenprüfung**.

Web-Schutz

Nur bei WLAN (auch über die **Mobile-Einstellungen** des Administrators): Der Web-Schutz ist nur aktiv, wenn eine WLAN-Verbindung besteht.

Fernadministration

Fernadministration gestatten: Erlaubt MobileSecurity durch den G Data ManagementServer administriert zu werden.

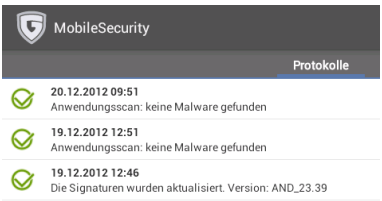
Serveradresse: Geben Sie hier die IP-Adresse oder den Servernamen des G Data ManagementServers an.

Gerätename: Geben Sie hier den Gerätenamen an.

Passwort: Geben Sie hier das Passwort ein, welches dazu verwendet wird, das mobile Gerät beim G Data ManagementServer zu authentifizieren (das Passwort wird im G Data Administrator im Bereich **Server-Einstellungen** definiert).

Protokolle

Der Bereich **Protokolle** erlaubt Ihnen, Einblick in Berichte zu nehmen, wie z.B. Virenprüfungs-Reports oder Reports zum Signatur-Update. Wählen Sie einen Protokolleintrag aus, um sich Details anzeigen zu lassen. Das Erstellen von Protokollen kann im Bereich **Einstellungen** an- oder abgeschaltet werden.

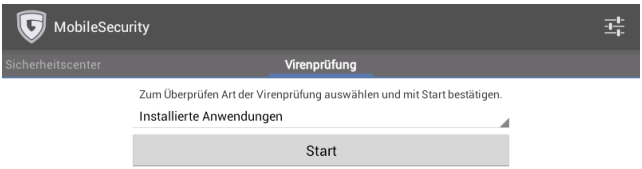


Module

Virenprüfung

Wählen Sie im Sicherheitscenter unter Virenprüfung einfach aus, welche Art der Virenprüfung stattfinden soll und klicken Sie dann auf Start, wenn Sie unabhängig von der automatischen Prüfung Ihr Gerät manuell überprüfen wollen.

- **Installierte Anwendungen**: Hier werden Ihre Apps mit einer ständig aktualisierten Liste von Schadsoftware verglichen. Wenn Sie tatsächlich Schadsoftware (Malware) auf Ihrem Gerät haben sollten, haben Sie dann direkt die Möglichkeit, die jeweilige Anwendung zu deinstallieren.
- **Gesamtes Smartphone inkl. SD-Karte**: Hier wird der gesamte Smartphone-Speicher auf Malware überprüft. Damit können Sie z.B. schädliche Applikationen auf der SD-Karte scannen, bevor Sie überhaupt installiert werden.

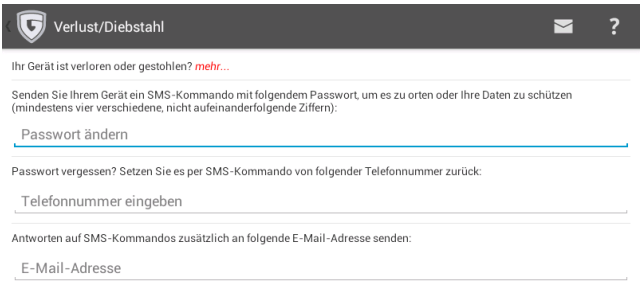


Klicken Sie auf die **Einstellungen**-Schaltfläche oben rechts im Programmfenster, um automatische und periodische Scan-Vorgänge zu definieren. Bitte beachten Sie, dass diese Einstellungen auch ferngesteuert im **Mobile-Einstellungen** des G Data Administrators vorgenommen werden können:

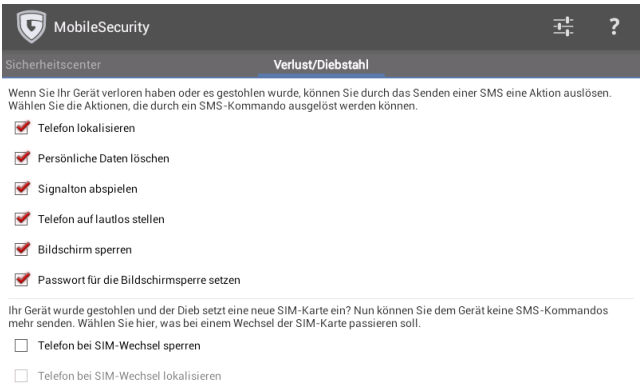
- **Automatische Prüfung**: Hier können Sie festlegen, dass neu installierte Applikationen automatisch überprüft werden.
- **Periodische Virenprüfung:** Hier können Sie einen periodischen Scan definieren.
- **Akkusparmodus**: Hier können Sie festlegen, dass der periodische Scan auch im Akkusparmodus durchgeführt wird.
- **Im Ladevorgang scannen**: Hier können Sie festlegen, dass der periodische Scan nur dann durchgeführt wird, wenn sich das Mobilgerät im Ladezustand befindet.
- **Scan-Häufigkeit**: Legen Sie hier die Scan-Periode fest (zwischen **1**, **3**, **7**, **14** oder **30** Tagen).
- **Art der Virenprüfung**: Legen Sie hier fest, ob nur eine Schnellprüfung der installierten Apps durchgeführt werden soll oder ein umfangreicher System-Scan.

Verlust/Diebstahl

Um verlorene oder gestohlene Mobilgeräte zu schützen, bietet die MobileSecurity verschiedene Maßnahmen an, die ferngesteuert über SMS aktiviert werden können. Wenn Sie das erste Mal das Menü **Verlust/Diebstahl** öffnen, werden Sie aufgefordert, ein **Passwort**, Ihre **Telefonnummer** und **E-Mail-Adresse** anzugeben.


Verlust/Diebstahl
Ihr Gerät ist verloren oder gestohlen? mehr...
Senden Sie Ihrem Gerät ein SMS-Kommando mit folgendem Passwort, um es zu orten oder Ihre Daten zu schützen (mindestens vier verschiedene, nicht aufeinanderfolgende Ziffern):
Passwort ändern
Passwort vergessen? Setzen Sie es per SMS-Kommando von folgender Telefonnummer zurück:
Telefonnummer eingeben
Antworten auf SMS-Kommandos zusätzlich an folgende E-Mail-Adresse senden:
E-Mail-Adresse

Das Passwort (ein Zahlen-PIN-Code) ist notwendig, damit Sie sich per SMS bei Ihrem Smartphone identifizieren können. Auf diese Weise wird verhindert, dass andere Personen unauthorisiert Sperrbefehle oder dergleichen an Ihr Gerät senden. Dieses Passwort kann nur über eine weitere SMS von der Telefonnummer geändert werden, mit der sie angelegt wurde. Die E-Mail-Adresse ist notwendig, um Antworten und Informationen zurück zu erhalten, die durch die SMS-Kommandos ausgelöst wurden (z.B. Standortinformationen). Tippen Sie auf **Fertig** am oberen linken Rand des Bildschirms, um Ihre Einstellungen zu speichern. Falls nötig, bestätigen sie über **Aktivieren** die vorgenommenen Änderungen an den Administrationsrechten. Später können diese Einstellungen jederzeit wieder über das Icon **Einstellungen** geändert werden.


MobileSecurity
Sicherheitscenter
Verlust/Diebstahl
Wenn Sie Ihr Gerät verloren haben oder es gestohlen wurde, können Sie durch das Senden einer SMS eine Aktion auslösen. Wählen Sie die Aktionen, die durch ein SMS-Kommando ausgelöst werden können.
Telefon lokalisieren
Persönliche Daten löschen
Signalton abspielen
Telefon auf lautlos stellen
Bildschirm sperren
Passwort für die Bildschirmsperre setzen
Ihr Gerät wurde gestohlen und der Dieb setzt eine neue SIM-Karte ein? Nun können Sie dem Gerät keine SMS-Kommandos mehr senden. Wählen Sie hier, was bei einem Wechsel der SIM-Karte passieren soll.
Telefon bei SIM-Wechsel sperren
Telefon bei SIM-Wechsel lokalisieren

Hier können Sie festlegen, welche Aktionen mit Ihrem Smartphone ausgeführt werden, sobald Sie diesem ein SMS-Kommando zuschicken. Setzen Sie hierzu Häkchen bei den Funktionen, die Sie aktivieren möchten:

- **Telefon lokalisieren**: Hiermit können Sie die Position des gestohlenen/verlorenen Gerätes an die E-Mail-Adresse senden lassen, welche Sie vorher im Einstellungen-Bereich definiert haben. Zum Aktivieren dieses Kommandos verschicken Sie einen SMS mit dem Textinhalt: *password* **locate**.
- **Persönliche Daten löschen:** Hiermit können Sie Ihr gestohlenes/verlorenes Handy auf den Werkszustand zurücksetzen. Alle persönlichen Daten werden dabei gelöscht. Zum Aktivieren dieses Kommandos verschicken Sie einen SMS mit dem Textinhalt: *password* **wipe**.
- **Signalton abspielen**: Über diese Funktion kann permanent ein akustisches Signal abgespielt werden. Dies erleichtert das Auffinden eines verlorenen Handys. Zum Aktivieren dieses Kommandos verschicken Sie einen SMS mit dem Textinhalt: *password* **ring**.
- **Telefon auf lautlos stellen**: Wenn Sie nicht möchten, dass Ihr gestohlenes/ verlorenes Smartphone durch Klingel- oder Systemtöne auf sich aufmerksam macht, können Sie es hiermit lautlos stellen. Die Funktionalität des Signaltons zum Wiederfinden des Geräts wird dabei natürlich nicht beeinträchtigt. Zum Aktivieren dieses Kommandos verschicken Sie einen SMS mit dem Textinhalt: *password* **mute**.
- **Bildschirm sperren**: Hiermit können Sie den Bildschirm Ihres gestohlenen/ verlorenen Smartphones sperren. Eine Nutzung des Smartphones ist so nicht mehr möglich. Zum Aktivieren dieses Kommandos verschicken Sie einen SMS mit dem Textinhalt: *password* **lock**. Sollte kein Passwort vergeben worden sein, wird hier das Passwort verwendet, welches Sie im Bereich **Einstellungen** vergeben haben.
- **Passwort für die Bildschirmsperre setzen**: Damit Sie selber wieder Zugang zu Ihrem Smartphone erhalten, können Sie mit dieser Funktion ggf. das Passwort für die Bildschirmsperre neu vergeben, wenn Sie das alte Passwort nicht mehr kennen. Zum Aktivieren dieses Kommandos verschicken Sie einen SMS mit dem Textinhalt: *password* **set device password:** *devicepassword*.

Sollte Ihr Smartphone gestohlen worden sein und der Dieb eine neue SIM-Karte einsetzen, um das Gerät für sich zu nutzen, können Sie folgende Aktionen ausführen:

- **Telefon bei SIM-Wechsel sperren**: Sobald eine andere SIM-Karte eingelegt wird, als die, welche sich bei der Aktivierung der MobileSecurity app im Smartphone befand, wird der Zugriff auf das Telefon komplett gesperrt. Das Telefon ist nun nicht mehr zu verwenden. Sobald die originale SIM-Karte wieder eingesetzt wird, ist auch das Telefon wieder verwendbar.

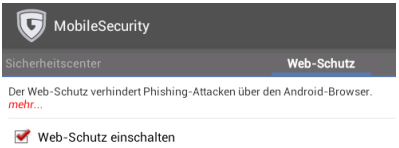
- **Telefon bei SIM-Wechsel lokalisieren**: Sobald die SIM-Karte gewechselt oder entfernt wird, wird Ihnen an die Mail-Adresse, die Sie im Einstellungen-Bereich angegeben haben, die aktuelle Position Ihres entwendeten Gerätes zugesandt.

Um das Passwort ferngesteuert zu ändern, senden Sie eine SMS mit dem Gerät an Ihr Handy, mit dem Sie zuvor das Passwort auch definiert haben. Das Kommand hierzu lautet: **remote password reset**: *password*.

Web-Schutz

Das Modul Web-Schutz schützt Sie vor Phishing-Attacken. Es blockt Phishing-Websites, so dass diese auf Ihrem Android-Browser nicht geöffnet werden können. Da der Web-Schutz immer auch ein gewisses Datenvolumen nach sich zieht, können Sie den Phishing-Schutz im **Einstellungen**-Bereich auch so einstellen, dass er nur dann aktiv ist, wenn Sie mit ihrem Smartphone WLAN nutzen.

Der Web-Schutz kann auch zentral über den Bereich **Mobile-Einstellungen** im G Data Administrator eingestellt werden.

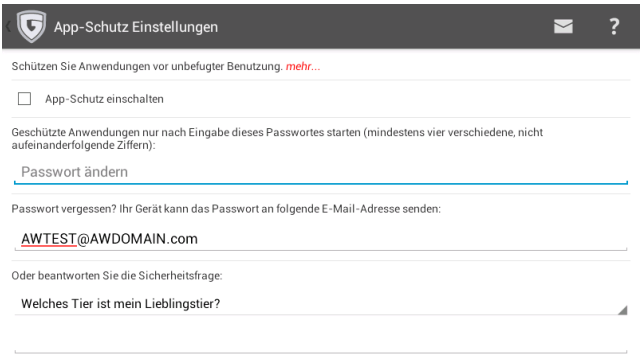


Berechtigungen

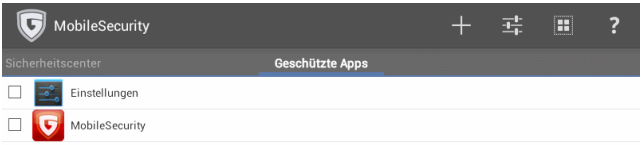
Im Bereich **Berechtigungen** haben Sie die Möglicheit, sich die Berechtigungen all Ihrer Apps anzeigen zu lassen und dann zu entscheiden, ob Sie eine App nicht vielleicht wieder löschen. Eine kostenlose Spiele-App, die auf das Adressbuch zugreift und SMS verschicken darf, sollte z.B. äußerst kritisch betrachtet werden. Wenn Sie einen Eintrag mit Berechtigungen antippen (z.B. **Anrufe** oder **Internetzugriff**) werden Ihnen alle Apps angezeigt, die diese Berechtigungen haben. Von hier aus können Sie Apps dann auch direkt deinstallieren.

App-Schutz

Über den App-Schutz können Sie bestimmte Apps auf Ihrem Smartphone vor unerlaubtem Zugriff schützen, so können Sie z.B. den Play-Store sperren, damit keine Apps ohne Ihre Erlaubnis gekauft werden. Wenn Sie das erste mal die App-Schutz Einstellungen aufrufen, werden Sie dazu aufgefordert, **Passwort**, **E-Mail-Adresse** und eine **Sicherheitsfrage** anzugeben.


App-Schutz Einstellungen
Schützen Sie Anwendungen vor unbefugter Benutzung. mehr...
App-Schutz einschalten
Geschützte Anwendungen nur nach Eingabe dieses Passwortes starten (mindestens vier verschiedene, nicht aufeinanderfolgende Ziffern):
Passwort ändern
Passwort vergessen? Ihr Gerät kann das Passwort an folgende E-Mail-Adresse senden:
AWTEST@AWDOMAIN.com
Oder beantworten Sie die Sicherheitsfrage:
Welches Tier ist mein Lieblingstier?

Das Passwort (ein PIN-Code) dient dazu, auf geschützte Anwendungen zugreifen zu können. Damit Sie ein vergessenes Passwort ggf. zurücksetzen können, sollten Sie eine E-Mail-Adresse angeben und eine Sicherheitsabfrage angeben. Das Passwort kann an die hier angegebene E-Mail-Adresse geschickt werden oder wird Ihnen, wenn Sie die Sicherheitsabfrage richtig beantworten (z.B. Mädchenname der Mutter, Name des Haustiers o.ä.) angezeigt. Drücken Sie nun auf die Schaltfläche **Speichern**.



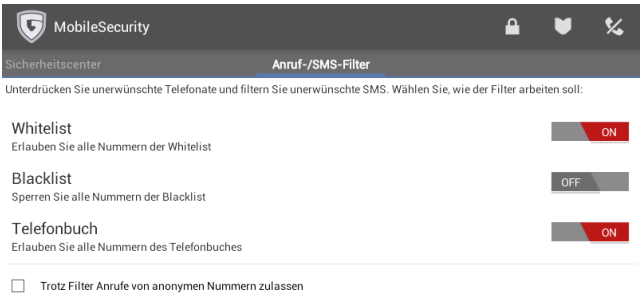
In der Hauptansicht des App-Schutz-Moduls sehen Sie eine Liste der geschützten Apps. Tippen Sie hier auf das + Symbol in der Titelzeile um die Apps auszuwählen, die Sie schützen möchten. Um eine App mit dem App-Schutz per Passwort zu schützen, setzen Sie einfach ein Häkchen vor die App. Genauso leicht können Sie den Schutz von Apps wieder abschalten, indem Sie das Häkchen vor der jeweiligen App hier entfernen.

Anruf-/SMS-Filter

Es gibt drei Möglichkeiten im Bereich Anruf-/(SMS-Filter bestimmte Absender für Anrufe und SMS zu filtern:

- **Whitelist**: Nur Einträge auf dieser Liste werden durchgestellt
- **Blacklist**: Einträge auf dieser Liste werden unterdrückt
- **Telefonbuch**: Nur Einträge im Telefonbuch werden durchgestellt.

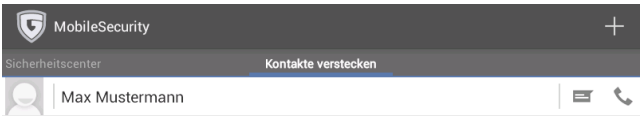
Die Filterliste **Telefonbuch** lässt sich mit der White- oder Blacklist kombinieren. Optional können anonyme Anrufe durchgestellt/unterdrückt werden, indem das Häkchen bei **Trotz Filter Anrufe von anonymen Nummern zulassen** gesetzt wird.



Um Einträge auf der Black- oder Whitelist anzuschauen, tippen Sie auf das Schloss-Icon. Um eine Telefonnummer zur Liste hinzuzufügen, tippen Sie auf das Plus-Icon. Telefonnummern können aus dem Adressbuch oder der Anrufhistorie ausgewählt werden.

Kontakte verstecken

Kontakte und ihre eingehenden Anrufe und Nachrichten können verborgen werden. Dazu verschieben Sie den jeweiligen Kontakt in einen geschlossenen G Data-Account im Modul **Kontakte verstecken**.



Wählen Sie die **Kontakte verstecken**-Option um eine Liste der momentan versteckten Kontakte anzuzeigen. Um einen Kontakt hier hinzuzufügen, tippen Sie bitte auf das Plus-Symbol. Sie können hierzu jeden Kontakt aus Ihrem Adressbuch oder der Telefonhistorie wählen. Nachdem der Kontakt in die Liste aufgenommen wurde, können Sie Einstellungen vornehmen, indem Sie den Namen des Kontaktes antippen. Um eingehende Nachrichten und Anrufe zu verbergen, wählen Sie **Kommunikation verbergen**. Um einen Kontakt aus dem Adressbuch zu verbergen, wählen Sie **Kontakte verbergen**. Verborgene Nachrichten können über die Auswahl von **Nachrichtenverlauf** oder **Anrufhistorie** angezeigt werden. Um einen Kontakt wieder anzuzeigen, wählen Sie ihn bitte aus und tippen auf **Eintrag löschen**. Der Kontakt wird dann aus dem verborgenen Bereich wieder in Ihr öffentliches Adressbuch übertragen.

FAQ

Installation

Nach der Installation des Clients laufen einige Anwendungen erheblich langsamer als vorher

Der Wächter überwacht im Hintergrund alle Dateizugriffe und prüft im Zugriff befindliche Dateien auf Viren. Dieses führt normalerweise zu einer kaum spürbaren Verzögerung. Falls eine Anwendung sehr viele Dateien oder einige Dateien sehr oft öffnet, kann eine erhebliche Verzögerung auftreten. Um dies zu umgehen, deaktivieren Sie den Wächter zunächst temporär, um herauszufinden, ob die Verzögerungen durch ihn hervorgerufen werden. Wenn der betroffene Rechner auf Dateien eines Servers zugreift, muss auch der Wächter auf dem Server temporär deaktiviert werden. Falls der Wächter die Ursache ist, kann das Problem i.d.R. durch die Definition einer Ausnahme (Dateien, die nicht geprüft werden sollen) behoben werden. Dazu müssen zunächst die Dateien ermittelt werden, auf die häufig zugegriffen wird. Mit einem Programm wie z.B. MonActivity können diese Daten ermittelt werden. Wenden Sie sich hierzu ggf. an unser **ServiceCenter**.

> Selbstverständlich können Sie auch die Performance dadurch steigern, indem Sie nicht beide Engines zur Virenüberprüfung verwenden, sondern nur eine Engine. Dies bietet sich in erster Linie auf älteren Systemen an und kann im **Wächter-Bereich** eingestellt werden.

Ich habe die G Data Software ohne Registrierung installiert. Wie kann ich die Software registrieren?

Um die Software nachträglich zu registrieren, öffnen Sie unter **Start** > **Alle Programme** > **G Data** > **G Data ManagementServer** das **Internet-Update**. Dort steht die Option **Online-Registrierung** zur Verfügung. Nach einem Klick auf diese Schaltfläche öffnet sich das Registrierungsformular. Geben Sie dort die Registriernummer ein, die dem Produkt beiliegt. Sie finden diese je nach Art des Produktes auf der Lizenzurkunde (MediaPack) oder in der Auftragsbestätigung. Kontaktieren Sie im Zweifelsfall Ihren Händler bzw. den betreuenden Distributor.

Durch die Eingabe der Registrierungsnummer wird Ihr Produkt aktiviert. Die erstellten Zugangsdaten werden Ihnen nach erfolgter Registrierung angezeigt. **Notieren Sie sich unbedingt diese Zugangsdaten!** Nach erfolgter Registrierung ist eine erneute Eingabe des Lizenzschlüssels nicht mehr möglich. Sollten Sie bei der Eingabe der Registriernummer Probleme haben, überprüfen Sie die Registriernummer auf die korrekte Eingabe. Je nach verwendeten Schriftsatz wird ein großes "I" (wie Ida) oft als die Ziffer "1", bzw. dem Buchstaben "l" (wie Ludwig) fehlinterpretiert. Das Gleiche gilt für: "B" und "8", "G" und 6, "Z" und "2".

> Sollten Sie eine G Data ClientSecurity, eine G Data EndpointProtection oder als Zusatzmodul einen G Data PatchManager erworben und bei der Installation nicht aktiviert haben, werden die Karteireiter Firewall, PatchManager und PolicyManager erst nach erfolgreicher Aktivierung freigeschaltet. Bis dahin stehen nur die Funktionen von G Data AntiVirus Business zur Verfügung.

MailSecurity, Exchange Server 2000 und AVM Ken!

Wenn Sie AVM Ken! nutzen und die G Data MailSecurity auf demselben Computer wie den Ken!-server installieren möchten, wenden Sie sich bitte an unser **Support-Team** für detaillierte Informationen.

Wenn Sie den Exchange Server 2000 nutzen und die G Data MailSecurity auf demselben Computer wie den Exchange Server installieren möchten oder wenn Sie die Ports für ein- und ausgehende Mails auf dem Exchange Server ändern möchten, wenden Sie sich bitte an unser **Support-Team** für detaillierte Informationen.

Fehlermeldungen

Client: "Programmdateien wurden verändert oder sind beschädigt"

Um einen optimalen Virenschutz zu gewährleisten, werden die Programmdateien regelmäßig auf Ihre Integrität geprüft. Bei einem Fehler wird der Bericht **Programmdateien wurden verändert oder sind beschädigt** eingefügt. Löschen Sie den Bericht und laden Sie das aktuelle Update der Programmdateien (G Data Client) von unserem Server. Führen Sie anschließend auf den betroffenen Clients eine Aktualisierung der Programmdateien durch. Kontaktieren Sie unsere **telefonische Hotline**, wenn der Fehlerbericht erneut eingefügt wird.

Client: "Die Virendatenbank ist beschädigt."

Um einen optimalen Virenschutz zu gewährleisten wird die Virendatenbank regelmäßig auf Ihre Unversehrtheit geprüft. Bei einem Fehler wird der Bericht **Die Virendatenbank ist beschädigt** eingefügt. Löschen Sie den Bericht und laden Sie das aktuelle Update der Virendatenbank von unserem Server. Führen Sie anschließend auf den betroffenen Clients eine Aktualisierung der Virendatenbank durch. Kontaktieren Sie unsere **telefonische Hotline**, wenn der Fehlerbericht erneut eingefügt wird.

"Sie benötigen mindestens Microsoft Exchange Server 2007 SP1"

Sollten Sie die Fehlermeldung "Sie benötigen mindestens Microsoft Exchange Server 2007 SP1" erhalten, sind die Mindestvoraussetzungen für die Installation der G Data MailSecurity Exchange-Plugin nicht erfüllt. Für eine Installation wird mindestens Microsoft Exchange 2007 mit Servicepack 1 benötigt. Dieser muss vor der G Data MailSecurity installiert werden. Siehe hierzu auch **Installation** und **Systemvoraussetzungen**.

Linux

Linux-Fileserver Clients: Es wird keine Verbindung zum G Data ManagementServer aufgebaut / Signaturen werden nicht aktualisiert

1 Prüfen Sie ob die beiden Prozesse des G Data Linux-Clients laufen. Geben Sie im Terminal

linux:~# ps ax|grep av

ein. Sie sollte die Ausgaben

... Ssl 0:07 /usr/sbin/avkserver –daemon
... Ssl 0:05 /usr/sbin/avclient –daemon

erhalten. Sie können die Prozesse unabhängig von der eingesetzten Distribution mit

linux:~# /etc/init.d/avkserver start
linux:~# /etc/init.d/avclient start

starten und mit

linux:~# /etc/init.d/avkserver stop

linux:~# /etc/init.d/avclient stop

anhalten. Hierzu müssen Sie als Administrator (root) auf dem Linux-Rechner eingeloggt sein.

2 Sehen Sie sich die Log-Dateien an: Unter **/var/log/** befindet sich die Log-Datei **gdata_install.log**. In dieser Datei wird der Verlauf der Remote-Installation protokolliert. Im Verzeichnis **/var/log/gdata** befindet sich die Log-Datei **avkclient.log**. In dieser Log-Datei werden die Scan-Ergebnisse des Scanners **avkserver** und die Ausgaben des Prozesses **avclient** protokolliert, der die Verbindung zum G Data ManagementServer herstellt. Schauen Sie sich die Dateien an und suchen Sie nach Fehlermeldungen. Wenn Sie mehr Meldungen sehen möchten, können Sie in den Konfigurationsdateien **/etc/gdata/gdav.ini** und **etc/gdata/avclient.cfg** die Einträge für **LogLevel** auf den Wert **7** setzen.

Vorsicht: Hohe LogLevel erzeugen viele Meldungen und lassen die Log-Dateien schnell anwachsen. Setzen Sie die LogLevel im Normalbetrieb immer auf niedrige Werte!

3 Testen Sie den Scanner: Mit dem Kommandozeilen-Tool **avkclient** können sie die Funktion des Scanservers **avkserver** testen. Folgende Kommandos lassen sich ausführen:

linux:~$ avkclient avkversion - gibt Version und Updatedatum der Virensignaturen aus

linux:~$ avkclient version - gibt Version in Kurzform aus

linux:~$ avkclient scan:<file> - scannt die Datei <file> und gibt das Ergebnis aus

4 Sehen Sie sich die Konfigurationsdatei an: Unter **etc/gdata/avclient.cfg** finden Sie die Konfigurationsdatei des Remoteclients **avclient**. Kontrollieren Sie, ob die Adresse des Haupt-Management-Servers (MainMMS) korrekt eingetragen ist. Falls nicht, löschen Sie den falschen Eintrag und melden den Linux-Client über den G Data Administrator erneut an oder tragen Sie die Adresse des G Data ManagementServers direkt ein.

5 Testen Sie Ihre Freigaben: Der Virenschutz für die Samba-Freigaben wird durch den Eintrag **vfs objects = gdvfs** in der Samba-Konfigurationsdatei **/etc/samba/smb.conf** aktiviert. Steht der Eintrag in der Sektion **[global]**, so ist der Schutz für alle Freigaben aktiviert. Steht die Zeile in einer anderen Sektion, so gilt der Schutz nur für die entsprechende Freigabe. Sie können die Zeile testweise auskommentieren (eine Raute (#) voranstellen), um festzustellen, ob der Zugriff ohne den Virenschutz funktioniert. Falls nicht, suchen Sie zunächst den Fehler in Ihrer Samba-Konfiguration.

6 Linux Workstation Wächter: Prüfen Sie, ob der Wächter-Prozess **avguard** läuft:

linux:~# ps ax|grep avguard

Der Wächter benötigt die Kernel-Module **redirfs** und **avflt**. Sie können mit **lsmod** prüfen, ob die Module geladen sind: **lsmod|grep redirfs** und **lsmod| grep avflt**.

Die Module müssen für den von Ihnen verwendeten Kernel kompiliert sein. Dies erledigt das Dynamic Kernel Module System (DKMS), welches zusammen mit den passenden Kernel-Header-Paketen Ihrer Distribution installiert sein muss. Wenn das der Fall ist, kompiliert und installiert DKMS die Module automatisch. Sie finden die Logdatei des Wächters unter **/var/log/gdata/avguard.log**.

Sonstiges

Wie kann ich überprüfen, ob die Clients eine Verbindung zum G Data ManagementServer haben?

Die Spalte **Letzter Zugriff** im Aufgabenbereich **Clients** enthält den Zeitpunkt, an dem sich der Client zum letzten Mal beim G Data ManagementServer gemeldet hat. In der Standardeinstellung melden sich die Clients alle fünf Minuten beim G Data ManagementServer (wenn gerade keine Scanaufträge ausgeführt werden). Folgende Ursachen können für eine fehlgeschlagene Verbindung verantwortlich sein:

- Der Client ist ausgeschaltet oder vom Netzwerk getrennt.
- Es kann keine TCP/IP-Verbindung zwischen dem Client und dem G Data ManagementServer aufgebaut werden. Prüfen Sie die Netzwerkeinstellungen bzw. Portfreigaben.
- Der Client kann die IP-Adresse des Servers nicht ermitteln, d.h. die DNS Namensauflösung funktioniert nicht. Die Verbindung kann mit dem Befehl **telnet** über die Eingabeaufforderung überprüft werden. Am Server muss TCP Port 7161 erreichbar sein, am Client muss TCP Port 7167 bzw. TCP Port 7169 erreichbar sein. Prüfen Sie die Verbindung mit dem Befehl **telnet <SERVERNAME> <PORTNUMMER>**

  Beachten Sie, dass unter Windows Vista, Windows 7 sowie Server 2008 (R2) der telnet-Befehl standardmäßig nicht verfügbar ist. Aktivieren Sie daher die entpsrechende Windows-Funktion bzw. fügen Sie sie als neues Feature zum Server hinzu. Ist die Verbindung vom Client zum Server intakt, erscheint in der Eingabeaufforderung eine Sammlung kryptischer Zeichen. Wenn die

Verbindung vom Server zum Client intakt ist, erscheint ein leeres Eingabefenster.

Mein Postfach wurde in die Quarantäne geschoben

Dies passiert, wenn sich in dem Postfach eine infizierte Mail befindet. Zurückbewegen der Datei: Schließen Sie das Mailprogramm auf dem betroffenen Client und löschen Sie eine evt. neu angelegte Archivdatei. Öffnen Sie anschließend im G Data Administrator den zugehörigen Bericht und klicken Sie auf **Datei zurückbewegen**. Kontaktieren Sie bitte unseren **Support**, wenn das Zurückbewegen fehlschlägt.

Der MMS soll nicht über seinen Namen, sondern über die IP-Adresse angesprochen werden

Installation des G Data ManagementServers

Bei der Installation wird nach dem Servernamen gefragt. Der Name muss durch die IP-Adresse ersetzt werden. Sie können den Servernamen auch nachträglich durch die IP-Adresse ersetzen, wenn der G Data ManagementServer bereits installiert ist. Passen Sie dazu - je nach Ihrem System - einen dieser Registry-Einträge an:

HKEY_LOCAL_MACHINE\SOFTWARE\G DATA\AVK ManagementServer\ComputerName

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\G DATA\AVK ManagementServer \ComputerName

Aktivierung der Clients im G Data Administrator

Damit die Verbindung vom Server zu den Clients auch über die IP-Adresse hergestellt werden kann, müssen die Clients im G Data Administrator mit Ihrer IP-Adresse aktiviert werden. Das geht entweder von Hand oder durch **Active Directory Synchronization**.

G Data Client-Setup von der DVD

Wenn die Clients direkt von der DVD installiert werden, fragt das Installationsprogramm sowohl nach dem Servernamen als auch nach dem Computernamen. Geben Sie hier jeweils die IP-Adresse ein.

Speicherorte und Pfade

Virensignaturen G Data Security Client

- Windows XP / Server 2003 / Server 2003 R2: C:\Programme\Gemeinsame Dateien \G DATA\AVKScanP\AVAST5 bzw. BD
- Windows Vista / Windows 7 / Windows 8 / Server 2008 / Server 2008 R2 / Server 2012: C:\Programme (x86)\Common Files\G DATA\AVKScanP\AVAST5 bzw. BD

Virensignaturen G Data ManagementServer

- Windows XP / Server 2003 / Server 2003 R2: C:\Dokumente und Einstellungen\All Users\Anwendungsdaten\G DATA\AntiVirus ManagementServer\Updates
- Windows Vista / Windows 7 / Windows 8 / Server 2008 / Server 2008 R2 / Server 2012: C:\ProgramData\G DATA\AntiVirus ManagementServer\Updates

G Data Security Client-Quarantäne

- Windows XP / Server 2003 / Server 2003 R2: C:\Programme\Gemeinsame Dateien \G DATA\AVKScanP\QBase
- Windows Vista / Windows 7 / Windows 8 / Server 2008 / Server 2008 R2 / Server 2012: C:\Programme (x86)\Common Files\G DATA\AVKScanP\QBase

G Data ManagementServer-Quarantäne

- Windows XP / Server 2003 / Server 2003 R2: C:\Dokumente und Einstellungen\All Users\Anwendungsdaten\G DATA\AntiVirus ManagementServer\Quarantine
- Windows Vista / Windows 7 / Windows 8 / Server 2008 / Server 2008 R2 / Server 2012: C:\ProgramData\G DATA\AntiVirus ManagementServer\Quarantine

MMS-Datenbanken

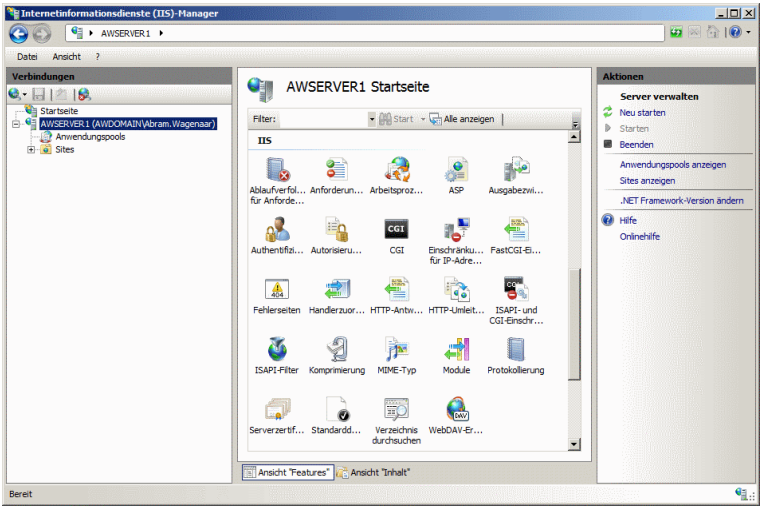
Windows XP / Windows Vista / Windows 7 / Windows 8 / Server 2003 / Server 2003 R2 / Server 2008 / Server 2008 R2 / Server 2012:

- C:\Programme\Microsoft SQL Server\MSSQL.1\MSSQL\Data \GDATA_AntiVirus_ManagementServer.mdf
- C:\Programme\Microsoft SQL Server\MSSQL.1\MSSQL\Data \GDATA_AntiVirus_ManagementServer_log.ldf

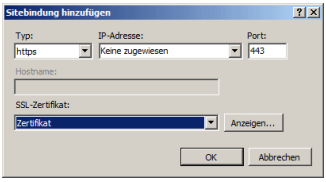
Wie aktiviere ich ein SSL-Server-Zertifikat in IIS 7 oder 7.5?

Um eine sichere Kommunikation zwischen Clients und WebAdministrator / MobileAdministrator zu erleichtern, empfiehlt es sich, ein SSL-Server-Zertifikat in Internet Information Services (IIS) zu ermöglichen.

Um ein SSL-Server-Zertifikat in IIS 7 oder 7.5 zu aktivieren, öffnen Sie bitte **Internetinformationsdienste (IIS)-Manager**. Wenn Sie Windows Server 2008 nutzen, können Sie den IIS Manager unter **Start** > **Alle Programme** > **Verwaltung** finden. Alternativ klicken Sie auf **Start** > **Ausführen** und geben Sie das Kommando *inetmgr* ein. Dieses Kommando kann auch auf Windows 7-Rechnern verwendet werden.



Wählen Sie Ihren Server unter **Verbindungen** aus. Wählen Sie dann die **IIS** Kategorie aus und doppelklicken auf **Serverzertifikate**. Klicken Sie nun auf **Selbstsigniertes Zertifikat erstellen**. Nach der Eingabe eines Namesn für das Zertifikat wird dieses erzeug und in der Serverzertifikat-Übersicht angezeigt. Bitte beachten Sie, dass das Standard-Ablaufdatum für das Zertifikat tagesgenau ein Jahr beträgt.

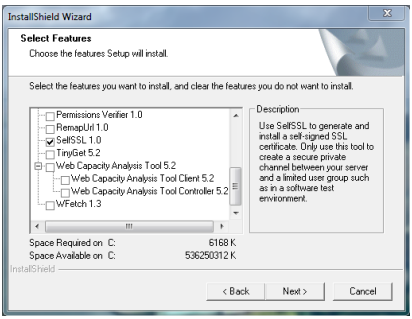


Um das Zertifkat für die Kommunikation zu verwenden wählen Sie die entsprechende Seite im Bereich **Verbindungen** aus. Im Bereich **Aktionen** auf der rechten Seite können Sie nun **Bindungen** auswählen. Klicken Sie nun auf **Hinzufügen**, um eine neue Bindung zu etablieren. Als **Typ** wählen Sie bitte *https* im DropDown-Menü aus und unter **SSL-Zertifikat** das Zertifikat, welches Sie zuvor definiert haben. Klicken Sie auf **OK**, um die Bindung zu bestätigen.

Der Zugriff auf den WebAdministrator und den MobileAdministrator über eine sichere Verbindung ist nun dadurch möglich, dass Sie das Präfix *http://*in Ihrem Browser durch *https://* ersetzen, z.B. *https://servername/gdadmin*. Da Sie Ihr Zertifikat selber erstellt haben, kann es sein, dass der Browser hier eine Warnung ausgibt, bevor er Ihnen erlaubt, den WebAdministrator oder MobileAdministrator zu öffnen. Trotzdem ist die Kommunikation mit dem Server vollständig verschlüsselt.

Wie aktiviere ich ein SSL-Server-Zertifikat in IIS 5 oder 6?

Um eine sichere Kommunikation zwischen Clients und WebAdministrator / MobileAdministrator zu erleichtern, empfiehlt es sich, ein SSL-Server-Zertifikat in Internet Information Services (IIS) zu ermöglichen.


InstallShield Wizard
Select Features
Choose the features Setup will install.
Select the features you want to install, and clear the features you do not want to install.
Permissions Verifier 1.0
RemapUrl 1.0
SelfSSL 1.0
TinyGet 5.2
Web Capacity Analysis Tool 5.2
Web Capacity Analysis Tool Client 5.2
Web Capacity Analysis Tool Controller 5.2
WFetch 1.3
Description
Use SelfSSL to generate and install a self-signed SSL certificate. Only use this tool to create a secure private channel between your server and a limited user group such as in a software test environment.
Space Required on C: 6168 K
Space Available on C: 536250312 K
InstallShield
< Back
Next >
Cancel

Um ein SSL-Server-Zertifikat in IIS 5 (Windows XP) oder IIS 6 (Windows Server 2003) zu aktivieren, verwenden Sie bitte das Microsoft-Tool *SelfSSL*, welches Sie bei den *IIS 6.0 Resource Kit Tools* (ein kostenloser Download von der **Microsoft website**) finden. Wenn Sie hier den Setup-Typ **Custom** durchführen, können Sie die Tools auswählen, die Sie installieren möchten. Wählen Sie hier bitte **SelfSSL 1.0** aus. Nach der Installation öffnen Sie die SelfSSL Kommandozeile über **Start** > **Programme** > **IIS Resources** > **SelfSSL**.

Mit Hilfe einer einzigen Eingabe können Sie nun ein selbst signiertes Zertifikat für Ihre Website erzeugen. Geben Sie bitte *selfssl /N:CN=localhost /K:2048 /V:365 /S:1 /T* ein und drücken Sie dann **Enter**. Bestätigen Sie die Erzeugung des Zertifikats durch Drücken der **Y**-Taste. Nun wird ein Zertifikat für die Standard-IIS Seite auf Ihrem lokalen Server erzeugt und der localhost wird auf die Liste der vertrauenswürdigen Zertifikate hinzugefügt.

Die Schlüssellänge beträgt 2048 Zeichen und ist für genau 365 Tage gültig. Wenn Ihre Seite nicht die Standard-ISS Seite auf Ihrem lokalen Server ist, können Sie unter **Start** > **Verwaltung** > **Internetinformationsdienste (IIS)-Manager** die entsprechende Seite auf Ihrem Server ermitteln und den Parameter */S:1* entsprechend modifizieren.

Der Zugriff auf den WebAdministrator und den MobileAdministrator über eine sichere Verbindung ist nun dadurch möglich, dass Sie das Präfix *http://*in Ihrem Browser durch *https://* ersetzen, z.B. *https://servername/gdadmin*. Da Sie Ihr Zertifikat selber erstellt haben, kann es sein, dass der Browser hier eine Warnung ausgibt, bevor er Ihnen erlaubt, den WebAdministrator oder MobileAdministrator zu öffnen. Trotzdem ist die Kommunikation mit dem Server vollständig verschlüsselt.

Index

A

Abholung 136
Absenderfilter 165
Aktivität 168
Aktualisieren 52
Alarmmeldungen 42
Allgemein 64
Anfragen 135
Anhänge filtern 163
Anruf-/SMS-Filter 178
AntiSpam 75
Anwendungskontrolle 89
App-Schutz 177
Aufgabenbereiche 53
Aufträge 78
Ausgehend 139
Ausgehend (SMTP) 134

B

Backup 47
Backupaufträge definieren 85
Beenden 38
Begrenzung 144
Benutzerkonto 150
Benutzerverwaltung 37
Berechtigungen 177
Berichte 105, 119
Blacklist 153

C

CD/DVD Boot-Option im BIOS einstellen 14
Clientauswahlbereich 49
Client-Einstellungen 63
Clients 55, 120

D

Dashboard 54, 118
Deaktivierte Clients anzeigen 52

E

Eingehend 138
Eingehend (POP3) 135
Eingehend (SMTP) 132
Einstellungen 43, 103, 145, 147, 171
E-Mail 71
E-Mail Einstellungen 45
Empfang 133, 134
Empfängerfilter 165
Erste Schritte 8
Erweitert 144
Externe Referenzen deaktivieren 162

F

Fehlermeldungen 181
Filter 136, 151, 160
Firewall 94, 127

G

G Data Administrator 32
G Data AntiVirus Business 140
G Data BootCD 12
G Data Business 3
G Data MailSecurity Administrator 130
G Data MailSecurity MailGateway 128
G Data ManagementServer 31
G Data MobileAdministrator 116
G Data MobileSecurity 170
G Data Security Client 122
G Data WebAdministrator 114
G Data BootCD erstellen 14
G Data Business-Lösungen 4
G Data Client Installationspaket erstellen 53
G Data MailSecurity Administrator konfigurieren 131
G Data Security Client deinstallieren 59
G Data Security Client installieren 59
Gerätekontrolle 91
Greylist-Filter 163
Größenbegrenzung 143
Gruppe bearbeiten 52

H

Hardware Inventar 61
Hilfe 49
Hilfe-Dokumentation 4
HTML-Skripte deaktivieren 162

I

Info 127
Inhaltsfilter 156, 165
Installation 7, 180
Installation der G Data MailSecurity 26
Installation der G Data MobileSecurity 29
Installation der G Data Security Clients 21
Installation des G Data Administrators 18
Installation des G Data ManagementServers 15
Installation des G Data MobileAdministrators 20
Installation des G Data WebAdministrators 19
Installation von Linux-Clients 24
Internet-Ambulanz 5
Internet-Einstellungen 149
Internetnutzungszeit 93
Internet-Update 38, 127
IP-Filter 166

K

Kennwort ändern 145
Kontakte verstecken 179

L

Lastbegrenzung 46
Lesebestätigung filtern 162
Linux 182
Lizenzmanagement 48
Logging 146
Lokale Installation 23
Löschen 53

M

Mobile-Einstellungen 76

N

Nachrichten 60
Neue Gruppe anlegen 52
Neue Reportplanung hinzufügen 110
Nicht zustellbare Nachrichten 143

O

Optionen 125, 132
Organisation 51

P

Patches 104
PatchManager 101
PolicyManager 89
Port-Konfiguration 10
PremiumHotline 5
Profi-Einstellungen 157
Programmbereiche 157
Programmdateien 150

Programmdateien (Client) 40
Programm-Updates 48
Protokoll anzeigen 36
Protokolle 172

Q

Quarantäne 126

R

Realtime Blacklists 154
Rechnername 144
Regelsätze 97
Remote-Installation 21
ReportManager 109, 121

S

Scanaufträge definieren 81
Scanparameter 140
Schlüsselwörter (Mailtext) 155
Schüsselwörter (Betreff) 154
Schutz vor Relaying 133
Server verwalten 37
Server-Einrichtungsassistent 34
Software Inventar 62
Softwareerkennung definieren 87
Softwareverteilung definieren 88
Sonstiges 184
Spam filtern 166
Spam-Filter 150
Sprachenfilter 166
Starten des G Data Administrators 33
Starten des G Data MailSecurity Administrators 131
Starten des G Data MobileAdministrators 116
Starten des G Data WebAdministrators 114
Statistik 113
Status 158
Subnet-Server-Synchronisation 38
Synchronisation 45
Systemnachrichten 145
Systemvoraussetzungen 10

T

Tray-Icon 122

U

Übersicht 56, 95, 101
Update 147
Update-Rollback Engine A/B 43
Updates/Patches 124

V

Verlust/Diebstahl 174
Verwendung des G Data MobileAdministrators 117
Verwendung des G Data WebAdministrators 115
Virendatenbank 39
Virenfunde 169
Virenprüfung 122, 137, 173
Virensignaturen 150

W

Wächter 67
Wächter ausschalten 125
Warteschlange 142
Warteschlangen 167
Web/IM 74
Web-Inhaltskontrolle 92
Web-Schutz 176
Weiterleitung 133, 135
Whitelist 152

Z

Zeitplanung Viren-Update 148
Zugangsdaten 147
Zugangsdaten und Einstellungen 41

Notizen